2022

Anti-Money Laundering and Combatting the Financing of Terrorism

GUIDELINES FOR DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

BANKING COMMISSION
THE REPUBLIC OF MARSHALL ISLANDS

Table of Contents

1. Introduction

These Guidelines are issued by the Banking Commissioner, as the supervisor of Designated Non-Financial Businesses and Professions (DNFBPs), pursuant to Section 12 of the Anti-Money Laundering Regulations 2002 (hereinafter "the AML Regulations 2002"). The Banking Commissioner is vested with responsibility for determining the compliance of DNFBPs with the AML Regulations 2002 and the Banking Act 1987.

1.1 Purpose and Scope

The purpose of these Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Guidelines for DNFBPs (hereinafter "the Guidelines") is to provide guidance and assistance to the supervised entities that are defined as DNFBPs under section 10(a)(1) of the revised AML Regulations 2002, to assist them in their better understanding and effective performance of the statutory obligations under the legal and regulatory framework in force in the Republic of Marshall Islands (hereinafter "RMI").

These Guidelines set out the minimum expectations of the Banking Commissioner, as an AML/CFT supervisory authority, regarding the factors that should be taken into consideration by each of the supervised DNFBPs when identifying, assessing, and mitigating the risks of money laundering (ML) and terrorist financing (TF).

Nothing in these Guidelines is intended to limit or otherwise restrict any additional or supplementary guidance, circulars, notifications, memoranda, communications, or other forms of guidance or feedback, whether direct or indirect, which may be published on occasion by the Banking Commissioner in respect of the supervised entities which fall under its AML/CFT supervision, or in respect of any specific supervised entity.

Finally, it should be noted that guidance on the subject of the United Nations Targeted Financial Sanctions (TFS) regime, and the related United Nations Sanctions (Implementation) Act 2020 and United Nations Targeted Financial Sanctions (Terrorism and Proliferation) Regulations 2020, as in force in the RMI, is outside of the scope of these Guidelines.

1.2 Applicability

Unless otherwise noted, these Guidelines apply to all DNFBPs, as defined under section 10(a)(1) of the revised AML Regulations 2002, and the members of their boards of directors, management, and employees, established and/or operating in the territory of RMI. Specifically, these Guidelines apply to all such natural and legal persons who fall into the following categories:

- Casinos;
- Real estate agents;
- Dealers in precious metals and dealers in precious stones;
- Lawyers, notaries, and other independent legal professionals;
- Accountants;
- Trust and company servicer providers (TCSPs); and
- Any other DNFBPs, as classified so by the AML Regulations 2002.

1.3 Legal Status of these Guidelines

These Guidelines do not constitute additional legislation or regulation and are not intended to set a legal, regulatory, or judicial precedent. They are intended to be read in conjunction with the relevant

laws, cabinet decisions, regulations, and regulatory rulings which are currently in force in the RMI. Supervised entities are reminded that the Guidelines do not replace or supersede any legal or regulatory requirements or statutory obligations. In the event of a discrepancy between these Guidelines and the legal or regulatory frameworks currently in force, the latter will prevail. Specifically, nothing in these Guidelines should be interpreted as providing any explicit or implicit guarantee or assurance that the Banking Commissioner or other competent authorities would defer, waive, or refrain from exercising their enforcement, judicial, or punitive powers in the event of a breach of the prevailing laws, regulations, or regulatory rulings.

These Guidelines, and any lists and/or examples provided in them, are not exhaustive and do not set limitations on the measures to be taken by supervised entities to meet their statutory obligations under the legal and regulatory framework currently in force in the RMI. As such, these Guidelines should not be construed as legal advice or legal interpretation. Supervised entities should perform risk assessments of how they should meet their statutory obligations, and they should seek legal or other professional advice if they are unsure of the application of the legal or regulatory frameworks to their particular circumstances.

1.4 Structure of the Guidelines

These Guidelines are divided into eight sections, which are as follows:

1. Introduction
2. Overview of the AML/CFT Legal and Regulatory Framework
3. Offenses of Money Laundering and Terrorist Financing
4. Identification and Assessment of ML/TF Risks
5. AML/CFT Governance, Internal Policies, Controls, Procedures, and Training
6. Customer Due Diligence
7. Suspicious Activity Reporting
8. Recordkeeping

Each section and sub-section of the Guidelines include references to the sections of AML Regulations 2002 to which it pertains. The text from the AML Regulations is either quoted or otherwise summarised or paraphrased, at various places through these Guidelines. In case of any inconsistency or discrepancy between the text provided in the AML Regulations 2002 and quotations, summaries, or paraphrases used in these Guidelines, the former shall prevail.

In cases, where the AML Regulations 2002 are deemed to be sufficiently clear concerning the statutory obligations of the DNFBPs, no additional guidance on those sections is provided in these Guidelines. However, guidance is provided with regards to subjects where more information or guidance is considered relevant for the DNFBPs to ensure their compliance with the AML Regulations, or on the subjects which are addressed either implicitly or by reference to international best practices in the AML Regulations 2002.

An attempt has been made to avoid the repetition of content in the Guidelines; however, it has sometimes become necessary to provide clarity to each section or sub-section, to make it comprehensive, and to minimize the need for cross-referencing.

These Guidelines will be updated or amended from time to time by the Banking Commissioner, as and when it is deemed appropriate. DNFBPs should bear in mind that these Guidelines are not the only source of guidance on the assessment and arrangement of ML/TF risks. There is guidance material available from several other international and regional organizations, such as Financial Action Task Force (FATF), Asia-Pacific Group on Money Laundering (APG), and other FATF-style regional bodies

(FSRBs), which DNFBPs are encouraged to refer to and consult in carrying out their statutory obligations. It is the sole responsibility of each DNFBP to keep itself apprised and updated on the ML/TF risks to which it is exposed, to maintain appropriate risk identification, assessment, and mitigation programs, and to ensure that their responsible personnel is adequately informed and trained on the relevant internal policies, procedures, and controls.

1.5 Terminology

The Guidelines use “must,” “should” and “may” throughout to contextualize how to understand the various directions. The terms have the below meanings:

- Must – a requirement in legislation or a requirement of a regulation or other mandatory provision. You must comply unless there are specific exemptions or defenses provided for in relevant legislation or regulations.

- Should – good practice for most situations. These may not be the only means of complying with the requirements and there may be situations where the suggested route is not the best option.

  If you do not follow the suggested route, you should be able to justify to supervisors why your alternative approach is appropriate, either for your practice or in the particular instance.

- May – an option for meeting your obligations or running your business or profession. Other options may be available and which option you choose is determined by the nature of the individual business, customers, or other matters. You may be required to justify why this was an appropriate option to the Banking Commissioner.

2. Overview of the AML/CFT Legal and Regulatory Framework

2.1 International Framework

The FATF is an inter-governmental body established in 1989, which sets out global standards and promotes effective implementation of legal, regulatory, and operational measures to combat ML, TF, proliferation financing, and other related threats to the integrity of the international financial system.[1] The FATF also monitors the implementation of its standards – the 40 Recommendations and 11 Immediate Outcomes, by applying the 'FATF Methodology' to assess the technical compliance of its members and members of FSRBs with the FATF Recommendations and the effectiveness of their AML/CFT systems.[2]

The FATF also publishes guidance on the risk-based approach to AML/CFT, including sector-specific guidance, for DNFBPs. The FATF standards and the FATF guidance are updated from time to time to keep abreast with the emerging ML/TF trends and typologies. The FATF guidance, including sector-specific guidance, can be accessed from the FATF website: https://www.fatf-gafi.org/

2.2 National Legal and Regulatory Framework

The AML/CFT legislative framework of the RMI is set out in the Banking Act 1987 and the AML Regulations 2002. The Banking Act 1987 and the AML Regulations 2002 have recently been revised and updated in 2021 to ensure compliance with the international AML/CFT standards, particularly the FATF Recommendations.

The amended AML Regulations 2002 obliges DNFBPs to put in place an effective, risk-based AML/CFT framework, which includes the application of a risk-based approach, AML/CFT governance, internal policies, procedures, controls and training, customer due diligence ("CDD") measures, reporting of suspicious transactions, requirements on higher-risk countries, and record keeping.

The Banking Commissioner is designated as a competent authority for the supervision and monitoring of the compliance of DNFBPs with the AML Regulations 2002 and is responsible for taking reasonable measures to ensure such compliance.

2.3 National AML/CFT Priorities

The RMI has completed its first National Risk Assessment (NRA) on ML/TF in August 2020. The NRA has identified the domestic threats, sectorial vulnerabilities (an overview of financial institutions and DNFBP sectors exposed to ML/TF), functional vulnerabilities (vulnerabilities that impact functions to combat ML/TF), and overarching vulnerabilities (cross-cutting vulnerabilities across the functional and sectoral vulnerability framework). Risks are analyzed as the function of likelihood and consequence of the nexus of the threats and vulnerabilities.

On reviewing all the threats and vulnerabilities, the NRA has identified five areas of urgent concern to the RMI's AML/CFT program regarding which action should be taken urgently. These five priority areas for developing and implementing immediate mitigating strategies are as follows:

- Priority 1 – Review the resourcing of the RMI's Financial Intelligence Unit (FIU) and ensure an adequate and effective AML/CFT supervisory program.
- Priority 2 – Resourcing of law enforcement and other operational agencies in the RMI AML/CFT program.

[1] See, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html
[2] See, https://www.fatf-gafi.org/publications/mutualevaluations/documents/fatf-methodology.html

- Priority 3 – Develop and implement systems to collect and record statistics and other data collection relevant to ML/FT.
- Priority 4 – Consider the development and implementation of a law relating to Proliferation Financing (PF).
- Priority 5 – Review, update and where necessary develop, the policies and procedures of the Trust Company of the Marshall Islands (TCMI) and its registries to ensure that the identified risks ML/FT/PF risks are mitigated.

3. Money Laundering and Terrorist Financing

3.1 Money Laundering

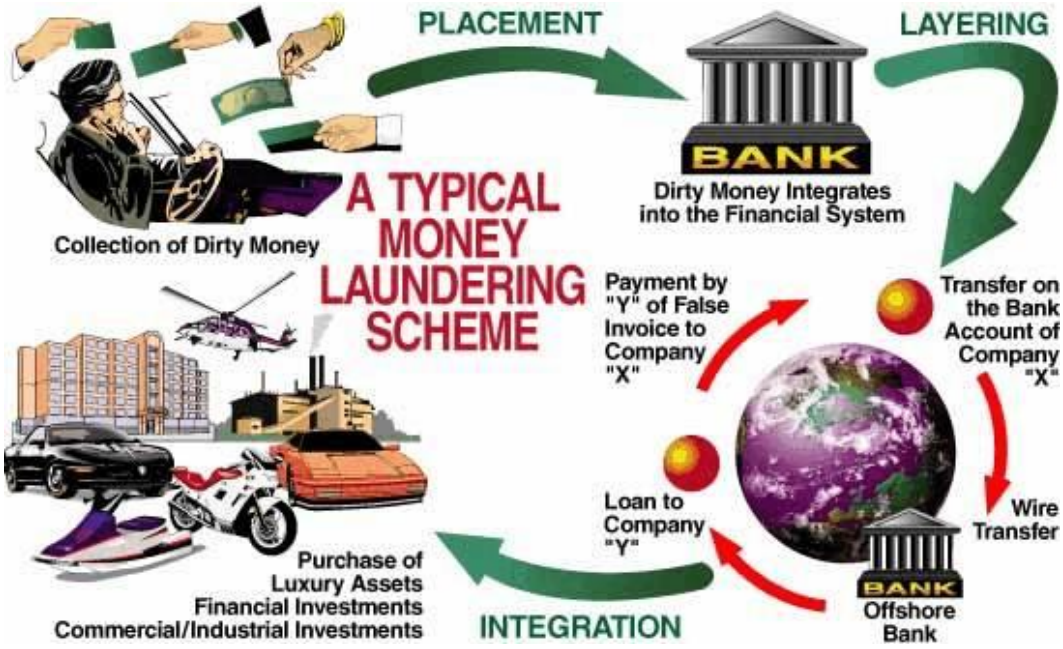
3.1.1. What is Money Laundering?

Money Laundering is generally defined as a process by which the proceeds of crime, or the true ownership of those proceeds, are changed or disguised so that they appear to come from a legitimate source. The FATF has defined 'money laundering' as the processing of criminal proceeds to disguise their illegal origin as legitimate ill-gotten gains of crime. In simple words, it is a process by which the dirty money (the proceeds of crime) is "washed" and turned into clean money.

3.1.2. Stages of Money Laundering

There are three acknowledged stages of the process of money laundering:

1. **Placement** – Placement is a process by which the proceeds of crime are disposed-off - this is how "dirty money" gets into the economy. This happens, for example, through cash deposits, cash conveyancing transactions, "smurfing", "hawala" systems, or smuggling assets.
2. **Layering** - Layering is a process by which money is passed through a lot of complex transactions to hide its origin. The techniques involve, for example, opening "off shore" or "shell" companies under false identifications, forged invoices, inflated invoice payments, or false loan repayments to launder the proceeds of crime.
3. **Integration** – Integration is the final stage of money laundering through which the dirty money that has been cleaned in the process is put back into the financial system as "clean money" after its origin has been obscured. The techniques involve, for example, the purchase of assets, such as real estate, bank notes, or luxury goods.



Source: United Nations Office on Drugs and Crime (UNODC)

The three stages of money laundering may occur as separate and distinct phases or may also occur simultaneously or may overlap.

It is important to note here that the stages of money laundering are not the legal concepts nor the elements of a money laundering offense. Placement, layering, and integration are just the terms used to describe the process, but from the legal point of view, the definition of the money laundering offense, as provided in the Banking Act 1987, will state the essential elements of the offense which needs to be proved in the court to secure a conviction for money laundering.

3.1.3. Money Laundering Offenses

Money laundering offenses are set out under Section 166 of the Banking Act 1987 (amended in 2020).

Section 166(1) of the Banking Act 1987 (as amended in 2020) provides that:

"*a person commits the offence of money laundering if the person intentionally:*

- *(a) acquires, possesses or uses property, knowing or having reason to believe that the property is the proceeds of crime;*
- *(b) converts or transfers property, knowing or having reason to believe that the property is the proceeds of crime, renders assistance to another person for the purpose of:*
  - *(i) concealing or disguising the illicit origin of that property or*
  - *(ii) aiding and abetting any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action; or*
- *(c) conceals or disguises the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing or having reason to believe that the property is the proceeds of crime."*

Section 166(4) of the Banking Act 1987 provides that "*a person who attempts, facilitates, conspires or aids and abets any other person to commit an offense of money laundering commits an offence and is liable on conviction to the penalties specified under [the] section."*

"Proceeds of crime" is defined in Section 1(x) of the Banking Act 1987. This definition encompasses all "serious offenses" as defined under section 1(dd) of the Banking Act 1987 (as amended in 2020).

Section 1(x) of the Banking Act 1987 defines proceeds of crime as including *"any property derived from or obtained directly or indirectly through the commission of a serious offense."*

Section 1(dd) of the Banking Act 1987 defines "serious offense" as "*an offense against a provision of:*

- *(i) any law in the Republic for which the maximum penalty is imprisonment or other deprivation of liberty for a period of not less than 12 months or imposition of a fine of $5,000 or more; or*
- *(ii) a law of a foreign State, in relation to acts or omissions, which, had they occurred in the Republic, would have constituted an offense for which the maximum penalty is imprisonment or other deprivation of liberty for a period of not less than 12 months or imposition of a fine of $5,000 or more.*

3.2 Terrorist Financing

Terrorist financing means an offense under Section 120(1) of the Counter Terrorism Act 2002.

Section 120(1) of the Counter Terrorism Act (CTA) 2002 provides that the offence of terrorist financing is committed if:

(1) Any person … knowingly, by any means, directly or indirectly, solicits, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part:

(a) for terrorism;

(b) for the benefit of persons who engage in terrorism, or for the benefit of entities owned or controlled, directly or indirectly, by persons who engage in terrorism; or

(c) for the benefit of persons and entities acting on behalf of or at the direction of any person referred to in subsection 1(b) …

Section 120(2) of the CTA 2002 provides that "*for an act to constitute an offense [of terrorist financing] it shall not be necessary that the funds were actually used to commit or carry out a terrorist offence or terrorist act.*"

Section 120(3) of the CTA 2002 prohibits anyone from making any funds, financial assets or economic resources or financial or other related services available, directly or indirectly to any persons referred to in subsection (1)(b) and (1)(c) of the section 120 above.

4. Identification and Assessment of AML/CFT Risks

4.1 Risk-based Approach (RBA)

DNFBPs are required to apply a RBA to the implementation of their AML/CFT Program.

A RBA is a process that allows DNFBPs to identify, assess and understand the ML and TF risks to which they are exposed and develop strategies including AML/CFT measures commensurate with those risks to manage and mitigate them effectively and proportionately.

The principle of RBA allows DNFBPs to allocate their resources more effectively and apply preventive measures that are commensurate with the nature and level of risks, to focus their AML/CFT efforts most effectively.

Senior management is ultimately responsible for making management decisions related to policies, procedures, and processes that mitigate and control the risks of ML and TF within a business. The scope of applied measures for prevention and detection of ML and TF should be proportionate to the identified level of ML and TF risk.

4.1.1 Assessing Business-level ML/TF risks

An important first step in applying a RBA is to identify, assess and understand the ML/TF risks by way of business-level ML/TF risk assessment. The key purpose of A business-level ML/TF risk assessment is to improve the effectiveness of ML/TF risk management through the identification of the general and specific ML/TF risks to which a DNFBP is exposed, determination of how these risks are mitigated by the controls embedded in DNFBP's AML/CFT Program and establishing the residual risk that remains for the DNFBP.

An effective business-level ML/TF risk assessment can allow DNFBPs to identify gaps and opportunities for improvement in their framework of internal AML/CFT policies, procedures, and controls, as well as to make informed management decisions about risk appetite, allocation of AML/CFT resources, and ML/TF risk-mitigation strategies that are appropriately aligned with residual risks. The assessment must be commensurate with the nature, size, and complexity of the financial institution's business.

The first step of conducting an ML/TF business risk assessment for DNFBPs is to identify, assess, and understand the inherent ML/FT risks (i.e., the risks that a DNFBP is exposed to if there were no control measures in place to mitigate them) across all business lines and processes concerning the following risk factors: customers, products, services and transactions, delivery channels, geographic locations, and any other risk factors.

With the inherent risks as a basis, the DNFBP can determine the nature and intensity of risk mitigating controls to apply to the inherent risks. The level of inherent ML/FT risks influences the kinds and levels of AML/CFT resources and mitigation strategies that DNFBPs require to put in place. The assessment of inherent ML/FT risks and the effectiveness of the risk mitigation measures will result in a residual risk assessment, i.e., the risks that remain when effective control measures are in place. In case the residual risk falls outside the risk appetite of a DNFBP, additional control measures will need to be implemented to ensure that the level of ML/FT risk is acceptable to the DNFBP.

DNFBPs should decide on both the frequency and methodology of business-level ML/FT risk assessments, including baseline and follow-up assessments, that are appropriate to their particular circumstances, taking into consideration the nature of the inherent and residual ML/FT risks to which they are exposed, as well as the results of the national risk assessment and any sectoral or thematic risk assessments. In most cases, DNFBPs should consider performing such risk assessments annually;

however, assessments that are more frequent or less frequent may be justified, depending on the particular circumstances. They should also decide on policies and procedures related to the periodic review of their business-level ML/TF risk assessment methodology, taking into consideration changes in internal or external factors. These decisions must be documented, approved by senior management, and communicated to the appropriate levels of the organization.

The result of an effective business-level ML/TF risk assessment will be the classification of identified risks into different categories, such as high, medium, low, or some combination of those categories (such as medium-high, medium-low). Such classifications may assist DNFBPs to prioritize their ML/FT risk exposures more effectively, so that they may determine the appropriate types and levels of AML/CFT resources needed and adopt and apply reasonable and risk-proportionate mitigation measures.

4.1.2 Risk Factors

Section 10(1) of the AML Regulations 2002 sets out the risk factors that DNFBPs are required to take into account when conducting their business-level risk assessment. The risk factors must be relevant to the DNFBP's business and include consideration of at least the following: customers, countries or geographical areas, products and services, type of transactions carried out, delivery channels, reliance on third parties, and new products, practices, and technologies

The sections below discuss various risk factors that DNFBPs must identify and assess as a part of their business-level ML/TF risk assessment, including:

- Customer risk;
- country or geographical risk
- products, services, and transactions risk;
- delivery channels risk;
- other risk factors; and
- new products, practices, and technology risk.

4.1.3 Customer Risk

When identifying the risk associated with their customers, including beneficial owners, DNFBPs should consider the risks related to:

- the industry, business, or professional activity of the customer and beneficial owner(s);
- the reputation of the customer and beneficial owner(s) in so far as it informs the DNFBP about the customer's or beneficial owner's financial crime risk; and
- the nature and behavior of the customer and beneficial owner(s), including whether this could indicate an increased TF risk.

4.1.3.1 Customer's Industry, Business, or Professional Activities

DNFBPs should consider the risk factors associated with the industry, business, or professional activities of a customer or customer's beneficial owner(s) including, for example, (recognizing that each of these factors will not be relevant to every customer), whether the customer or its beneficial owner:

- Has political connections, for example:
    - the customer or its beneficial owner is a Politically Exposed Person ("PEP") or has any other relevant links to a PEP; or
    - one or more of the customer's directors are PEPs and if so, these PEPs exercise significant control over the customer or beneficial owner; or

- has links to sectors that are commonly associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, arms trade and defense, extractive industries, and public procurement;
- has links to sectors that are particularly susceptible to ML or TF risk; for example, certain money service businesses or casinos;
- has links to sectors that involve significant amounts of cash;
- is a legal person or a legal arrangement and if so, the purpose of their establishment and the nature of their business;
    - holds another prominent position or enjoys a high public profile that might enable them to abuse this position for private gain. For example, they are:
        - senior public officials with the ability to influence the awarding of public contracts;
        - individuals that are known to influence the government and other senior decision-makers; or
    - is a public body or state-owned entity from a jurisdiction with high levels of corruption.

Other risk factors that DNFBPs may consider about a customer's industry, business, or professional activity include, for example, whether:

- a customer is a legal person subject to enforceable disclosure requirements that ensure that reliable information about the customer's beneficial owner is publicly available. For example, a public company listed on a regulated market or other trading platforms that makes such disclosure a condition for listing and/or admission to trading;
- the customer is a credit or financial institution acting on its account from a jurisdiction with an effective AML/CFT regime. For example, whether:
    - It is supervised for compliance with local AML/CFT obligations; and
    - If so supervised, there is no evidence that the customer has been subject to supervisory sanctions or enforcement for failure to comply with AML/CFT obligations or wider conduct requirements in recent years; or
- the customer's background is consistent with the DNFBPs's knowledge about it. This includes, for example:
    - its former, current, or planned business activity;
    - the turnover of the business;
    - its source of funds; and
    - the customer's or beneficial owner's source of wealth.

4.1.3.2 Customer's Reputation

Risk factors that DNFBPs should consider, where appropriate, when assessing the risks associated with a customer's or beneficial owner's reputation include, for example, whether:

- there are adverse media reports or other relevant information sources about the customer or its beneficial owner. For example, there are reliable and credible allegations of criminality or terrorism against the customer or their beneficial owners. DNFBPs should determine the credibility of allegations inter alia based on the quality and independence of the source data and the persistence of reporting of these allegations. DNFBPs should note that the absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing;
- the customer, beneficial owner, or anyone publicly known to be closely associated with them has currently, or had in the past, their assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorist financing ;
- the customer or beneficial owner has been the subject of a suspicious transactions report by the DNFBP in the past; or

- the DNFBP has in-house information about the customer's or their beneficial owner's integrity, obtained, for example, in the course of a long-standing business relationship.

4.1.3.3 Nature and Behaviour of Customer and Customer's Beneficial Owner

Risk factors that DNFBPs should consider, where appropriate, when assessing the risk associated with the nature and behavior of a customer's or customer's beneficial owner include, for example, whether:

- the customer is unable to provide robust evidence of their identity;
- the DNFBP has doubts about the veracity or accuracy of the customer's or beneficial owner's identity;
- the customer's ownership and control structure appears unnecessarily complex or opaque and there is no obvious commercial or lawful rationale for such structures;
- the customer has nominee shareholders, where there is no obvious reason for having these;
- the customer issues shares in bearer form;
- the customer is a special purpose vehicle ("SPV") or structured finance company where beneficial ownership is not transparent;
- the customer is a high net worth customer, especially if the source of funds is unclear;
- there are frequent or unexplained changes to a customer's legal, governance, or beneficial ownership structures (e.g., to its board of directors);
- the customer requests transactions that are complex, unusually or unexpectedly large or have an unusual or unexpected pattern without apparent economic or lawful purpose or a sound commercial rationale;
- there are grounds to suspect that the customer is trying to evade specific thresholds such as those set out for occasional transactions under the AML Regulations 2002;
- the customer requests unnecessary or unreasonable levels of secrecy. For example, the customer is reluctant to share CDD information, or appears to disguise the true nature of its business;
- the customer's or beneficial owner's source of wealth or source of funds cannot be easily and plausibly explained. For example, through its occupation, inheritance, or investments;
- the customer does not use the products and services it has taken out as expected when the business relationship was first established;
- the customer is a non-resident and its needs could be better serviced elsewhere. For example, there is no apparent sound economic and/or lawful rationale for the customer requesting the type of service sought in RMI;
- the customer is a non-profit organization whose activities put them at a heightened risk of being abused for terrorist financing purposes;
- the customer is a beneficiary of a life insurance policy; or
- the customer is insensitive to price or significant losses on investments.

Risk factors associated with the nature and behavior of customers or beneficial owners, which may indicate an increased TF risk, especially when other TF risk factors are also present may include, whether:

- the customer or beneficial owner is publicly known to be under investigation for terrorist activity or has been convicted for terrorist activity or is known to have close personal or professional links to such persons;
- the customer performs transactions involving the incoming and outgoing fund transfers from and/or to countries where groups committing terrorist offenses are known to be operating;
- the customer is a not-for-profit organization:
    - whose activities or leadership have been publicly known to be associated with extremists or terrorist sympathizers; or

- whose transaction behavior involves bulk transfers of large amounts of funds to jurisdictions associated with higher ML/TF risk and high-risk third countries;
- whose transactions are characterized by large flows of money in a short period, involving non-profit organizations with unclear links;
- who intends to transfer funds to:
  - named persons included on lists of persons, groups, or entities involved in terrorist acts and subject to UN Sanctions or are known to have close personal or professional links to persons registered on such lists; or
  - persons, groups, or entities publicly known to be under investigation for terrorist activity or who have been convicted for terrorist activity or are known to have close personal or professional links to such persons.

4.1.4 Country or Geographic Risk

Country or Geographic Risk relates to:

- jurisdictions in which the customer is based or where the customer and beneficial owner is resident;
- jurisdictions which are the customeŕs and beneficial owner's main places of business; and
- Jurisdictions to which the customer and beneficial owner appear to have relevant personal or business links, legal or financial interests, of which the DNFBP should reasonably have been aware.

When identifying the risk associated with countries and geographic areas, DNFBPs should consider, for example, the risk factors related to:

- the nature and purpose of the business relationship within the jurisdiction;
- the effectiveness of the jurisdiction's AML/CFT regime;
- the level of predicate offenses relevant to money laundering within the jurisdiction;
- the level of TF risk associated with the jurisdiction; and
- any economic or financial sanctions against a jurisdiction

4.1.4.1 Nature and Purpose of the Business Relationship within the Jurisdiction

The nature and purpose of the business relationship will often determine the relative importance of the individual country and geographic risk factors. The risk factor that DNFBPs should consider, where appropriate, including for example:

- where the funds used in the business relationship have been generated abroad, the level of predicate offenses relevant to money laundering, and the effectiveness of the country's legal system;
- where funds are received from or sent to jurisdictions where groups committing terrorist offenses are known to be operating, the extent to which this is expected or might give rise to suspicion is based on what the DNFBP knows about the purpose and nature of the business relationship;
- where the customer is a credit or financial institution, the adequacy of the country's AML/CFT regime and the effectiveness of AML/CFT supervision; or
- for customers other than natural persons, the extent to which the country in which the customer (and where applicable, the beneficial owner/s) is registered, effectively complies with international tax transparency standards.

4.1.4.2 Effectiveness of Jurisdiction's AML/CFT Regime

Risk factors that DNFBPs should consider when assessing the risk associated with the effectiveness of a jurisdiction's AML/CFT regime include, for example, whether:

- the country has been identified by FATF as having strategic deficiencies in its AML/CFT regime;

- there is information from one or more credible and reliable sources about the quality of the jurisdiction's AML/CFT controls, including information about the quality and effectiveness of regulatory enforcement and oversight. Examples of possible sources include:
    - Mutual Evaluations of the FATF or (FATF-style Regional Bodies);
    - the FATF's list of high risk and other monitored jurisdictions; and
    - International Monetary Fund assessments.

4.1.4.3 Level of Jurisdiction's Predicate Offences

Risk factors that DNFBPS should consider when assessing the risk associated with the level of predicate offenses relevant to money laundering in a jurisdiction include, for example, whether:

- there is information from credible and reliable public sources about the level of predicate offenses relevant to money laundering, for example, corruption, organized crime, tax crime, or fraud. Examples include corruption perceptions indices; OECD country reports on the implementation of the OECD's anti-bribery convention; and the UNODC World Drug Report; or
- there is information from more than one credible and reliable source about the capacity of the jurisdiction's investigative and judicial system effectiveness to investigate and prosecute these offenses.

4.1.4.4 Level of Jurisdiction's TF Risk

Risk factors that DNFBPs should consider when assessing the level of TF risk associated with a jurisdiction include, for example, whether:

- there is information, for example, from law enforcement or credible and reliable open media sources, suggesting that the jurisdiction provides funding or support for terrorist activities or that groups committing terrorist offenses are known to be operating in the country or territory; or
- there is information, for example, from law enforcement or credible and reliable open media sources, suggesting that groups committing terrorist offenses are known to be operating in the country or territory; or
- the jurisdiction is subject to financial sanctions, embargoes, or measures that are related to terrorism, financing of terrorism, or proliferation issued, for example, by the United Nations and the EU.

4.1.5 Product, Service, and Transaction Related Risk

Risk factors that DNFBPs should consider when assessing the risk associated with their products, services, or transactions, include, for example:

- The level of transparency, or opaqueness, the product, service, or transaction affords;
- The complexity of the product, service, or transaction; and
- The value or size of the product, service, or transaction.

4.1.5.1 Transparency of Products, Services, or Transactions Risk

Risk factors that DNFBPs should consider when assessing the risk associated with the transparency of products, services, or transactions include, where appropriate, for example:

- the extent to which products or services facilitate, or allow anonymity or opaqueness of customer, ownership, or beneficiary structures that could be used for illicit purposes, for example, bearer shares, offshore and certain trusts, or cash transactions;
- non-face-to-face transactions;
- legal entities structured in a way to take advantage of anonymity;
- dealings with shell companies or companies with nominee shareholders;
- the extent to which is it possible for a third party that is not part of the business relationship to give instructions.

4.1.5.2 Complexity of Products, Services, or Transactions

Risk factors that DNFBPs should consider when assessing the risks associated with a product, service, or transaction's complexity include, where appropriate, for example:

- the extent that the transaction is complex and involves multiple parties or multiple jurisdictions, and conversely, the extent that the transaction is straightforward;
- the extent that the products or services allow payments from third parties. Where third-party payments are permitted, the extent to which the DNFBP can identify the third party and understands their relationship with the customer; and
- the risks associated with new or innovative products or services, in particular where this involves the use of new technologies or payment methods (see 4.1.8 of these Guidelines).

4.1.5.3 Value and Size of Products, Services, or Transactions

Risk factors that DNFBPs should consider when assessing the risk associated with the value or size of a product, service, or transaction include, where appropriate, for example:

- the extent that products or services may be cash intensive; and
- the extent that products or services facilitate or encourage high-value transactions, for example, there are no caps on certain transaction values or levels of payment that could limit the use of the product or service for money laundering or terrorist financing purposes.

4.1.6 Delivery/Distribution Channel Risk

When identifying the risk associated with the Delivery/Distribution channel, DNFBPs should consider the risk factors related to:

- the extent that the business relationship is conducted on a non-face-to-face basis; and
- any introducers or intermediaries a DNFBP utilizes and the nature of their relationship with the DNFBP.

4.1.6.1 How the Business Relationship is Conducted

Risk factors that DNFBPs should consider when assessing the risk associated with how the business relationship is conducted, including for example, whether:

- The customer is physically present for identification purposes. If they are not,
  - has the customer deliberately avoided face-to-face contact other than for reasons of convenience or incapacity;
  - whether the DNFBP uses reliable forms of non-face-to-face CDD; and
  - the extent that the DNFBP has taken steps to prevent impersonation or identity fraud.

Appendix 1 of the AML Regulations 2002 provides that non-face-to-face business relationships and transactions include but are not limited to:

a. business relationships concluded over the Internet or by other means such as through the post;
b. services and transactions over the Internet including trading in securities by retail investors over the Internet or other interactive computer services;
c. use of ATM machines;
d. mobile telephone banking;
e. transmission of instructions or applications via facsimile or similar means; and
f. making payments and receiving cash withdrawals as part of electronic point of sale transaction using prepaid or re-loadable or account-linked value cards.

4.1.6.2 Channels used to introduce Customers to the Firm

Risk factors that DNFBPs should consider when assessing the risk associated with customers introduced to the DNFBP include for example, whether:

- the customer has been introduced from other parts of the same legal entity or group and if so,
    - The extent that the DNFBP can rely on this introduction as reassurance that the customer will not expose the DNFBP to excessive ML/TF risk; and
    - the extent that the DNFBP has taken measures to satisfy itself that the group entity applies CDD measures equivalent to the AML Regulations 2002;
- the customer has been introduced by a third party that is not a part of the group entity.
- where the customer has been introduced by a third party, the extent of the measures that the DNFBP has undertaken to be satisfied whether:
    - a third party is a regulated person subject to AML/CFT obligations consistent with those set out under FATF Recommendations;
    - the third party is subject to licensing and effective AML supervision and there are no indications that the third party's level of compliance with applicable AML legislation or regulation is inadequate, for example, because the third party has been subject to any disciplinary actions or sanctioned for breaches of AML/CFT obligations;
    - the third party applies CDD measures and keeps records equivalent to the RMI requirements and that it is supervised for compliance with comparable AML/CFT obligations in line with AML Regulations 2002;
    - the third party will provide, immediately upon request, relevant copies of identification and verification data, among others in line with Section 3F.4 of the aml Regulations 2002;
    - the quality of the third party's CDD measures is such that it can be relied upon; and
    - the level of CDD applied by the third party is commensurate to the ML/TF risk associated with the business relationship.

4.1.6.3 Use of Intermediaries

Risk factors that DNFBPs should consider when assessing the risk associated with the use of intermediaries include for example, whether the intermediary is:

- a regulated person subject to AML obligations that are consistent with those of the FATF Recommendations;
- subject to effective AML supervision and there are no indications that the intermediary's level of compliance with applicable AML legislation or regulation is inadequate, for example, because the intermediary has been subject to disciplinary actions or sanctioned for breaches of AML/CFT obligations;
- involved on an ongoing basis in the conduct of business and whether this affects the DNFBP's knowledge of the customer and ongoing risk management;
- based in a jurisdiction associated with higher ML/TF risk. Where an intermediary is based in a high-risk third country that the FATF has identified as having strategic deficiencies, DNFBPs should not rely on that intermediary. Reliance may be placed on an intermediary where it is a branch or majority-owned subsidiary of another DNFBP, and the DNFBP is confident that the intermediary fully complies with group-wide policies and procedures.

4.1.7 Other Risk Factors

Given the ever-evolving nature of ML/FT risks, new risks are constantly emerging, while existing ones may change in their relative importance due to legal or regulatory developments, changes in the marketplace, or as a result of new or disruptive products or technologies. For this reason, no list of risks can ever be considered exhaustive.

Nevertheless, additional factors that may present specific risks are, e.g., the introduction of new products or services, new technologies or delivery processes, or the establishment of new branches and subsidiaries locally and abroad. To ensure, therefore, that DNFBPs are in a position to review and update the ML/TF business risk assessment as well as mitigation measures, DNFBPs should take into consideration the results of the NRA or any sectoral or thematic risk assessments. They should also consult publications from official sources regularly, including those of the Banking Commission, other competent or supervisory authorities, the FATF, APG and other FSRBs, the Egmont Group, and others. Links to some of these sources can be found in Annex 9.2

Examples of some of the types of additional risk factors which DNFBPs may consider in identifying and assessing their ML/FT risk exposure include:

4.1.7.1. Novelty/innovation

DNFBPs should consider the depth of experience with and knowledge of the product, service, transaction, or channel type. Products, services, transactions, or delivery channel types that are new to the market or the DNFBP may not be as well understood, and may therefore pose a different level of ML/FT risk than, more established ones. Likewise, products, services, transactions, or delivery channel types that are unexpected or unusual concerning a particular type of customer may indicate a different level of potential ML/FT risk exposure than would more traditional or expected product, service, transaction, or channel types regarding that same type of customer.

4.1.7.2. Cybersecurity/distributed networks.

DNFBPs may consider evaluating the degree to which their operational processes and/or their customers expose them to the risk of exploitation for professional third-party money laundering and/or the financing of terrorism, through cyber-attacks or other means, such as the use of distributed technology or social networks.

4.1.8 Assessing New Product, Practices, and New Technologies Risks

Section 10(a)(3) of the AML Regulations 2002 requires the DNFBPs to identify and assess the ML/TF risks that may arise in relation to development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. It states that DNFBPs "*must (a) undertake the risk assessment prior to the launch or use of such products, practices, and technologies; and (b) have policies in place and take such measures as are needed to manage and mitigate the risks*."

DNFBPs must complete the assessment of risks relating to new products, new business practices, and the use of new or developing technologies and take the appropriate risk management measures, before launching new products and services, practices or techniques, or technologies. In general, they should integrate these ML/FT risk assessment and mitigation requirements into their new product, service, channel, or technology development processes.

To assess the ML/FT risks associated with new products, services, practices, techniques, or technologies, DNFBPs may consider utilizing the same or similar risk assessment models or methodologies as those utilized for their business-level ML/TF risk assessments, updated as necessary for the particular circumstances. They should also document the new product, service, practice, technique, or technology risk assessments, in keeping with the nature and size of their businesses

4.2 Risk Assessment Methodology and Documentation

4.2.1 Risk Assessment Methodology

DNFBPs are obliged to document their business-level ML/TF risk assessments. DNFBPs may utilize a variety of models or methodologies in assessing their ML/FT risk. DNFBPs should determine the type and extent of the risk assessment methodology that they consider to be appropriate for the size and nature of their business, and should document the rationale for their decisions.

To be effective, a risk assessment should be based on a methodology that:

- is based on quantitative and qualitative data and information and makes use of internal meetings or interviews; internal questionnaires concerning risk identification and controls; review of internal audit reports;
- reflects the DNFBP's management-approved AML/CFT risk appetite and strategy;
- takes into consideration input from relevant internal sources, including input and views from the designated member of senior management, AML/CFT Compliance Officer, and other relevant units like risk management and internal control;
- takes into consideration relevant information (such as ML/FT trends and sectoral risks) from external sources, including the national risk or any sectoral or thematic risk assessment, any information or guidance provided by the Banking Commission, and the FATF, APG, and other FSRBs, the Egmont Group, and others where appropriate;
- describes the weighting of risk factors, the classification of risks into different categories, and the prioritization of risks.
- evaluates the likelihood or probability of occurrence of identified ML/FT risks, and determines their timing and impact on the DNFBP.
- takes into account whether the AML/CFT controls are effective, specifically whether there are adequate controls to mitigate risks concerning customers, products, services, or transactions.
- determines the effectiveness of the AML/CFT risk mitigating measures in place by using information such as audit and compliance reports or management information reports.
- determines the residual risk as a result of the inherent risks and the effectiveness of the AML/CFT risk mitigating measures.
- establishes based on the residual risk and the risk appetite, whether additional AML/CFT controls have to be put in place.
- determines the rationale and circumstances for approving and performing manual interventions or exceptions to model-based risk weightings or classifications.
- is properly documented and maintained, regularly evaluated and updated, and communicated to management and relevant personnel within the organization.
- is tested and audited for the effectiveness and consistency of the risk methodology and its output concerning statutory obligations.

4.2.1.1 Weighting Risk Factors

As part of their risk assessment methodology, DNFBP should consider whether to weigh risk factors differently depending on their relative importance.

When weighing risk factors, DNFBPs should make an informed judgment about, and document the relevance of different risk factors in the context of a business relationship or transaction. The weight given to each of these factors is likely to vary from product to product and customer to customer (or category of the customer) and from one DNFBP to another.

When weighing risk factors DNFBPs should ensure that:

- weighting is not unduly influenced by just one factor;

- economic or profit considerations do not influence the risk rating;
- weighting does not lead to a situation where no business relationship can be classified as higher-risk;
- situations identified by national legislation as always presenting a higher ML risk cannot be over-ruled by the DNFBP's weighting, for example, PEPs; and
- DNFBPs can override any automatically generated risk scores where necessary. The rationale for the decision to override such scores should be governed and documented appropriately.

Where DNFBPs use automated IT systems to allocate overall risk scores to categorize business relationships or transactions and do not develop this in-house but rather purchase them from an external provider, they should ensure that:

- the DNFBP fully understands the risk rating methodology and how it combines risk factors to achieve an overall risk score;
- The methodology used meets the DNFBP's risk assessment requirements and legal and regulatory obligations; and
- the DNFBP can satisfy itself that the scores allocated are accurate and reflect the DNFBP's understanding of ML/TF risk.

4.2.1.2 Categorizing Business Relationships and Occasional Transactions

Following their business-level ML/TF risk assessment, DNFBPs should categorize their business relationships and occasional transactions according to the perceived level of ML/TF risk. DNFBPs should decide on the most appropriate way to categorize risk, which may include low, medium, and high, or some combination of those categories (such as medium-high, medium-low). This generally depends on the nature and size of the DNFBP's business and the types of ML/TF risk to which it is exposed. Ideally, the risk categorization for business relationships and occasional transactions should be the same as used for business-level ML/TF risk assessment.

4.2.2 Documentation, Monitoring, and Updating of Business-level Risk Assessment

Section 10(3) of the AML Regulations 2002 requires that the DNFBPs must document their risk assessments in writing in a manner that demonstrates their basis, keep them up-to-date and provide them to the Banking Commissioner upon request.

4.2.2.1. Documenting Risk Assessment

Business-level ML/TF risk assessment conducted by DNFBPs must be documented. A well-documented assessment of the identified inherent risk factors is fundamental to the adoption and effective application of reasonable and proportionate ML/TF risk-mitigation measures. It allows for a systematic categorization and prioritization of inherent and residual ML/TF risks, which in turn allows DNFBPs to determine the types and appropriate levels of AML/CFT resources needed for mitigation purposes. Documented risk assessment also allows the risk assessment strategies to be shared with management and employees.

DNFBPs are obliged to document their business-level ML/TF risk assessment in writing in a manner that demonstrates their basis, which includes documenting methodology, analysis, and supporting data, and making them available to the Banking Commission upon request. DNFBPs should incorporate into their documentation, the information used to conduct the business-level ML/TF risk assessment to demonstrate the effectiveness of their risk assessment processes.

4.2.2.2. Monitoring the Emerging ML/TF Risks for Risk Assessment

DNFBPs must keep their business-level ML/TF risk assessment and assessments of the ML/TF risk associated with individual business relationships and occasional transactions as well as of the underlying factors under review to ensure their assessment of ML/TF risk remains up to date and relevant. Where a DNFBP is aware that a new risk has emerged, or an existing one has increased, this must be reflected in business-level ML/TF risk assessment as soon as possible

DNFBPs should ensure that they have systems and controls in place to identify emerging ML/TF risks and that they can assess these risks and, where appropriate, incorporate them into their business-level risk assessment on time.

Examples of systems and controls that DNFBPs should put in place to identify emerging risks include:

- Processes to ensure that internal information is reviewed regularly to identify trends and emerging issues;
- Processes to ensure that a DNFBP regularly reviews relevant information from sources such as:
    - The RMI's NRA;
    - NRA of the jurisdiction(s) in which the DNFBP operates or customers of a DNFBP is located;
    - Communications issued by the Banking Commissioner;
    - Guidance, circulars, and other communication from the Banking Commissioner and other relevant regulatory bodies ;
    - Information obtained as part of the initial CDD process;
    - DNFBP's own knowledge and expertise;
    - Information from industry bodies or associations;
    - Information from international standard-setting bodies such as Mutual Evaluation Reports("MERs") or thematic reviews;
    - Changes to terror alerts and sanctions regimes as soon as they occur, for example, by regularly reviewing terror alerts and looking for sanctions regime updates;
    - Information from international institutions and standard-setting bodies relevant to ML/TF risks (e.g. UN, IMF, Basel, FATF); and
    - Other credible and reliable sources that can be accessed individually or through commercially available databases or tools that are determined necessary by a Firm on a risk-sensitive basis;
- Processes to capture and review information on risks relating to new products;
- Engagement with other industry representatives, competent authorities, and the Banking Commissioner (e.g. round tables, conferences, and training providers), and processes to feed back any findings to relevant staff; and
- Establishing a culture of information sharing and strong ethics within the DNFBP.

4.2.2.3. Updating the Risk Assessment

DNFBPs should put in place systems and controls to ensure their business-level risk assessments remain up to date. Examples include:

- Setting a timeline on which the next risk assessment update will take place, to ensure changing, new, or emerging risks are included in risk assessments. Where the DNFBP is aware that a new risk has emerged, or an existing one has increased, this should be reflected in risk assessments as soon as possible;
- Carefully recording issues throughout the year that could have a bearing on risk assessments, such as:
    - Internal suspicious transaction reports;
    - Compliance failures and intelligence from front office staff; or

- Any findings from internal/external audit reports;

Like the original risk assessments, any update to a risk assessment and adjustment of accompanying CDD measures must be documented, proportionate, and commensurate to the ML/TF risk.

5. AML/CFT Governance, Internal Policies, Procedures, Controls, and Training

5.1 An Overview

The AML Regulations 2002 requires DNFBPs to adopt and implement internal policies, procedures, and controls to manage and mitigate ML/TF risks ("the AML/CFT Program"). The AML/CFT program of a DNFBP must be informed by its business-level ML/TF risk assessment and must have regard to matters such as the nature and size of its business. It must be risk-based and proportionate to the risks involved, as well as consistent with the results of their business-level ML/TF risk assessment and the requirements of the AML Regulations 2002. DNFBPs must also consider the results of both the NRA and any sectoral risk assessments to inform their AML/CFT program.

The AML/CFT program must be approved by the senior management, regularly monitored for effectiveness, and continuously updated and enhanced to mitigate the ML/TF risks as and when they are identified.

The internal policies, procedures, and controls that DNFBPs should design to prevent, detect and deter ML/TF risks can be categorized broadly as those related to:

- The identification and assessment of ML/TF risks (Section 4 of these Guidelines);
- Customer due diligence (CDD), including enhanced CDD and simplified CDD, including its review, updating, and reliance on third parties (Section 6 of these Guidelines);
- Customer and transaction monitoring and the reporting of suspicious transactions (Section 7 of these Guidelines);
- AML/CFT Governance, including senior management responsibilities, designated compliance function, independent auditing of risk mitigation measures, and training (section 5 below of these Guidelines);
- Record-keeping requirements (section 8 of these Guidelines)

Three lines of defense must be addressed in the AML/CFT Program of a DNFBP. These are:

- A system of internal policies, procedures, and controls, including an ongoing employee training program (first line of defense);
- A designated compliance function with a compliance officer (second line of defense); and
- An independent audit function to test the overall effectiveness of the AML/CFT Program (third line of defense).

In setting up these three lines of defense, DNFBPs can take into account the nature, size, and complexity of their business

5.2 Setting the tone at the top

The attitude and culture embedded within a DNFBP are of critical importance in the fight against money laundering and terrorist financing. DNFBPs should ensure that there is a strong compliance culture throughout the organization, in which the role of the board of directors ("Board") and senior management is crucial. There should be clear and simple high-level statements that are uniform across the organization, setting the risk appetite and ensuring a compliance culture that prevents a DNFBP from being abused by criminals.

DNFBPs should ensure that the AML/CFT roles and responsibilities of senior management are clearly defined and documented. Similarly, the roles and responsibilities of the Board and other relevant key

functions within the DNFBP, such as the member of the senior management with responsibility for AML/CFT matters (where relevant), the Compliance Officer with responsibility for AML/CFT (where relevant), and internal audit (where relevant), should also be clearly defined and documented concerning AML/CFT activities within the DNFBP.

5.3 Roles and Responsibilities of the Board

The Banking Commissioner expects the Board to demonstrate effective governance and oversight of the DNFBP's AML/CFT compliance framework.

This oversight should include, without being limited to, the following measures:

- AML/CFT Program: The Board should review and approve all AML/CFT policies, procedures, and controls of a DNFBP and ensures that they are timely reviewed and updated.
- Business-level risk assessments: The Board should:
    - review and approve the methodology used for undertaking a Business-level risk assessment of a DNFBP.
    - Review and approve the DNFBP's Business-level risk assessment at least on an annual basis to ensure that it is aware of the ML/TF risks facing the business and that the corresponding AML/CFT measures that the DNFBP has in place are commensurate with the level of ML/TF risk identified.
- Reporting Lines: The Board should ensure that appropriate reporting lines are in place to facilitate the escalation of AML/CFT issues from the Compliance Officer for discussion by the Board. The Compliance Officer should have a mechanism to communicate directly with the Board.
- Board Meetings: The Board should ensure that:
    - AML/CFT issues appear as an agenda item at regular intervals at a Board meeting(s) and the corresponding minutes reflect the level of discussion and outcomes, which took place concerning any AML/CFT management information provided by the Compliance Officer or any particular AML/CFT issues requiring discussion by the Board.
    - The Compliance Officer delivers a report to the Board at least on an annual basis and a detailed discussion on its content takes place with corresponding minutes to reflect the level of discussion.
- AML/CFT Resourcing: The Board should ensure that
    - The DNFBP's AML/CFT function is adequately resourced (both in terms of staff and systems) commensurate with the level of ML/TF risk faced by the DNFBP.
    - Reviews are undertaken on a regular and timely basis to consider whether the DNFBP has the appropriate staff numbers, the correct skill set and whether staff has access to adequate systems and other resources to effectively perform their role as it relates to AML/CFT issues.

DNFBPs should ensure that appropriate evidence of discussions at Board meetings and/or approvals concerning AML/CFT issues are recorded and retained in accordance with the DNFBP's record retention policy.

5.4 Identification of the Member of Senior Management

"Senior Management" is defined in Section a(18) of the AML Regulations 2002 as "*an officer or employee of the bank, FSP, or DNFBP with sufficient knowledge of its money laundering and terrorist financing risk exposure, and sufficient authority, to make decisions affecting its risk exposure*".

DNFBPs should appoint a member of senior management with primary responsibility for implementing, managing and monitoring DNFBP's AML/CFT Program, including ensuring its compliance with the AML/CFT measures, where such an appointment is proportionate to the nature, scale, and complexity of the DNFBP's activities.

This is a key measure to ensure that DNFBPs do not attach low priority to AML/CFT issues. A lack of understanding of AML/CFT matters at the senior management level can result in a corporate culture that pursues profits at the expense of a robust compliance framework. The Board should ensure that the person so appointed has adequate knowledge, skills, and experience regarding the identification, assessment, and management of the ML/TF risks, and the implementation of AML/CFT policies, controls, and procedures, in addition to a good understanding of the DNFBP's business model and the sector in which the DNFBP is operating, and the extent to which this business model exposes the DNFBP to ML/TF risks.

Where a DNFBP has decided that it is not necessary to appoint a member of senior management, having regard to the nature, scale, and complexities of the DNFBP's activities, it should record in detail its rationale for such a decision. In such circumstances, the DNFBP must ensure that it remains in compliance with all obligations under the AML Regulations 2002. This includes ensuring that all matters requiring approval by senior management are approved at the appropriate level.

5.5 Tasks and Role of the Member of Senior Management

The member of senior management has primary responsibility for the implementation, management, and monitoring of DNFBP's AML/CFT Program, including ensuring its compliance with the AML Regulations 2002. Accordingly, he/she should ensure that the Board is provided with relevant, adequate, and timely information regarding AML/CFT matters and is aware of the impact of ML/TF risks on the activities of the DNFBP. In effectively discharging this role, the tasks that should be carried out by the member of senior management include, but are not limited to, the following:

- Approval of the DNFBP's ML/TF Risk Assessment conducted under Section 10 of the AML Regulations 2002;
- Approval of any higher-risk customers or PEP relationships under sections 3K.2 and 3K.3;
- Approval of the DNFBP's AML/CFT Program adopted under section 2A.1;
- Ensuring that the Compliance officer:
    - has direct access to all the information necessary to perform his/her tasks;
    - has sufficient human and technical resources to execute all responsibilities effectively; and
    - is well-informed of the AML/CFT-related incidents highlighted by the internal control systems and of the shortcomings in implementing the AML/CFT provisions found by the national and, if relevant, foreign supervisory authorities.
- Ensuring that the audit functions are adequately resourced;
- Ensuring that remedial actions are taken on a timely basis on the recommendations made by internal and external auditors and supervisors concerning the DNFBP's AML/CFT program; and
- Ensuring that training is provided to all relevant categories of staff, including compliance officers, on an ongoing basis which enables them to effectively discharge their AML/CFT responsibilities.

5.6 Compliance Officer

Section 2A.2 of the AML Regulations 2002 provides that DNFBPs must designate an individual at management level as a 'Compliance Officer'. The Compliance Officer should be given timely access to customer identification data and customer due diligence (CDD) information, transaction records and any other relevant information.

5.6.1 Appointment and Approval

As per the requirements of the AML Regulations 2002, the Banking Commissioner expects DNFBPs to designate a member of staff at the management level as a 'Compliance Officer'. The Compliance officer should be responsible to monitor and manage compliance with, and for the internal communication of the DNFBP's internal AML/CFT policies, procedures, and controls, where appropriate, having regard to the nature, scale, and complexity of the DNFBP's activities.

DNFBPs should ensure that the person designated as Compliance Officer:

- must have sufficient and appropriate AML/CFT knowledge and expertise, including knowledge of the applicable legal and regulatory AML/CFT framework *i.e.,* the Banking Act 1987, the AML Regulations 2002, the National Risk Assessment, thematic and sector risk assessment, and any guidance or information on AML/CFT provided by the Banking Commission (Section 2A.3 of the AML Regulations), and the implementation of AML/CFT policies, controls, and procedures;
- must understand the powers of the Banking Commission and the penalties for non-compliance with the Banking Act and the AML Regulations 2002 (Section 2A.3 of the AML Regulations);
- has the autonomy and authority to act independently and to exercise sufficient influence within the DNFBP to allow him/her to discharge his/her duties effectively (Section 2A.2 of the AML Regulations 2002);
- is capable of providing effective challenge within the DNFBP on AML/CFT matters when necessary;
- has the capabilities, capacity, and experience to oversee the identification and assessment of suspicious transactions and to report/liaise with the relevant authorities where necessary concerning such transactions;
- sufficient knowledge and understanding of the ML/TF risks to which the business is exposed, with relevant experience regarding the identification, assessment, and management of such ML/TF risks;
- keeps up to date with current and emerging ML/TF trends and issues in the industry and understands how such issues may impact the DNFBP; and
- has unrestricted and direct access to adequate resources and all information that in the opinion of the Compliance Officer is necessary to allow him/her to discharge his/her duties effectively.
- is readily accessible to staff on AML/CFT matters.

5.6.2 Compliance Officer Reporting to the Board

Section 2A.2 of the AML Regulations 2002 provides that "*the Compliance Officer should have the authority to act independently and to report to senior management above the compliance officer's next reporting level or the Board of Directors or equivalent body*."

DNFBPs should ensure that there are adequate policies and procedures in place to ensure effective reporting and escalation of AML/CFT matters by the Compliance Officer to the Member of Senior Management, and to the Board, as appropriate.

Such reporting should include at least:

- Regular and timely AML/CFT management information, including concerning any matter requiring senior management approval under the AML Regulations 2002, regarding the AML/CFT activities at the DNFBP. Such information should be sufficiently detailed to ensure that the members of Senior Management, and the Board where appropriate, can make timely, informed and appropriate decisions on AML/CFT matters;

- a "Compliance Officer Report" on the DNFBP's AML/CFT activities. The Compliance Officer Report should*, inter alia*;
    - be produced, or reviewed and agreed, by the Compliance Officer at least on an annual basis;
    - be presented by the Compliance Officer to the Board on time;
    - be proportionate to the nature, scale, and complexities of the DNFBP's activities;
    - provide comments and feedback on the effectiveness of the DNFBP's AML/CFT systems and controls; and
    - include recommendations, as appropriate, for improvement in the management of the DNFBP's ML/TF risk.

5.6.3 Responsibilities of the Compliance Officer

The responsibilities of the Compliance Officer can be broadly grouped into the following categories:

- Suspicious Activity Reporting

  The Compliance Officer should be the DNFBP's officer-in-charge for reviewing, scrutinizing, and reporting SARs to the Banking Commissioner. In this capacity, the Compliance Officer is ultimately responsible for the detection and investigation related to ML and TF, for reporting suspicious transactions to the Banking Commissioner, and for cooperating with the Banking Commissioner and other competent authorities concerning the AML/CFT matters.

- The AML/CFT Program and related matters

  The Compliance Officer should be responsible for:
    - developing DNFBPs' internal policies, procedures, and controls that are approved by the Board;
    - carry out, or monitor the carrying out of, ongoing monitoring of all AML/CFT obligations of the DNFBPs. This implies sample testing of compliance to alert any non-adherence with the AML/CFT procedures to the Member of Senior Management or the Board;
    - reviewing and updating the AML/CFT Program on time in response to events or emerging risks, and ensuring that such updates are communicated to relevant staff on a timely basis;
    - establishing a clearly defined process in place for the formal review at least annually of the AML/CFT Program at appropriate levels, with approval where changes are material;
    - conducting periodic assessments and testing of the AML/CFT control mechanisms and systems to ensure their continued relevance and effectiveness in addressing changing ML/TF risks;
    - conducting DNFBP's ML/TF risk assessments including timely assessment of new products and services as well as new technology and processes;
    - ensuring system resources, including those required to identify and report suspicious transactions, are appropriate in all relevant areas of the DNFBP;
    - Ensure that internal policies and procedures are readily available to all staff and are fully implemented and adhered to by all staff;
    - informing employees and officers promptly of any regulatory and legislative changes and revisions to policies and procedures;
    - promoting compliance with the AML/CFT laws, regulations, and this Guideline, and taking overall charge of all AML/CFT matters within the DNFBP;
    - ensures that systems and other processes that generate information used in reports to Senior Management and the Board are adequate and appropriate, use reasonably consistent reporting criteria, and generate accurate information;
    - reporting to the Member of Senior Management on the outcome of reviews of the DNFBP's compliance with the AML/CFT laws, regulations and this Guidelines, and risk assessment procedures; and

- reporting regularly on key AML/CFT risk management and control issues, and any necessary remedial actions, arising from audit, inspection, and compliance reviews, to the DNFBP's senior management and the Board.

- AML/CFT Training and Development

  The Compliance Officer should be responsible for assisting to establish and maintain a strong and effective AML/CFT compliance culture within the DNFBP. This responsibility includes working with the designated member of senior management and other internal and external stakeholders to ensure that the DNFBP's staff are well-qualified, well-training, well-equipped, and well-aware of their responsibilities to combat the threat posed by ML/TF.

  The Compliance Officer should be responsible for ensuring that ongoing training programs on ML and TF are current and relevant and are carried out for all employees, senior management, and the Board.

The business interests of the DNFBP shall not interfere with the effective discharge of the above-mentioned tasks and responsibilities of the Compliance Officer, and potential conflicts of interest should be avoided. To ensure unbiased judgments and facilitate impartial advice to the Senior Management and the Board, the Compliance function should, for example, be distinct from the internal audit and business line functions. Where any conflict arises between business lines and the responsibilities of the Compliance Officer, there should be appropriate policies and procedures in place to ensure that AML/CFT concerns are objectively considered and addressed at the appropriate level of the DNFBP's management.

5.7 Screening of Employees

Section 2A.7 of the AML Regulations 2002 provides that the DNFBPs "*must have adequate screening procedures to ensure high standards when hiring employees. This must include identification of past convictions for offences involving dishonesty, financially-motivated crime or money laundering.*"

DNFBPs must ensure that the employees that they have recruited possess high ethical standards and integrity. Some of the factors that DNFBPs should take into consideration in this regard include, but are not limited to:

- obtaining and confirming appropriate references at the time of recruitment;
- requesting information from employees regarding any regulatory action taken against them or action taken by a professional body, and
- requiring information from employees concerning any criminal convictions and the provision of a check of their criminal record. The DNFBPs should also take steps to manage any potential conflicts of interest of employees with the AML/CFT responsibilities.

5.8 Financial Group-wide policies and procedures

Section a(11) of the AML Regulations 2002 defines a 'financial group' as "*a group of a parent company (or any other legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles), together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level*."

Section 9(b) of the AML Regulations further provides that:

"*Financial groups must implement group-wide AML/CFT programs applicable and appropriate to all branches and majority-owned subsidiaries of the financial group. These should include the measures set out in Section 2A and 2B.3 [of the AML Regulations 2002] and also:*

(1) policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management;

(2) the provision, at group-level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This should include information and analysis of transactions or activities which appear unusual (if such analysis was done). Similarly, branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management; and

(3) adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off."

Where applicable, the DNFBPs must ensure that they comply with obligations under the AML Regulations 2002 relating to financial group-wide policies and procedures. Adequate systems and mechanisms should be put into place to ensure their compliance with the financial group-wide requirements under the AML Regulations 2002.

5.9 Independent Audit Function

Section 2A.4 of the AML Regulations 2002 sets out the obligation of DNFBPs to maintain an adequately resourced and independent audit function to test compliance (including sample testing) with Part XIII of the Banking Act 1987 and the AML Regulations 2002.

Section 2B.3 of the AML Regulations 2002 further provides that DNFBPs "*shall ensure an annual independent audit is performed to verify the adequacy of, and compliance with , the AML /CFT Program. … DNFBPs shall submit to the Banking Commissioner the report resulting from the annual independent audit."*

Independent audit is required to be carried out by the DNFBPs in accordance with any guidance provided by the Banking Commission.

A robust and independent audit function is a key component of a well-functioning governance structure and an effective AML/CFT framework. DNFBPs are obliged to have in place an adequately resourced and independent audit function to test the effectiveness and adequacy of their internal

policies, procedures, and controls relating to combating the crimes of money laundering and terrorist financing. In this regard, DNFBPs should ensure that their independent audit function is appropriately staffed and organized and that it has the requisite competencies and experience to carry out its responsibilities effectively, commensurate with the ML/FT risks to which the DNFBPs are exposed, and with the nature and size of their businesses.

DNFBPs are required to perform the independent audit of their AML/CFT Program, including business-level ML/TF risk assessment and AML/CFT mitigation measures, and CDD policies, procedures, and controls, at least on an annual basis, and are also required to submit the findings of their annual audit report to the Banking Commissioner annually.

DNFBPs should ensure that the annual inspection and testing of all aspects of their AML/CFT Program are incorporated into their regular audit plans. They should also ensure that all their branches and the subsidiaries in which they hold a majority interest, whether domestic or foreign, are part of an independent audit testing program that covers the effectiveness and adequacy of their internal AML/CFT policies, controls, and procedures.

It should be noted that, while most DNFBPs are expected to have the capacity to meet these requirements internally, depending on the nature and size of their businesses, some DNFBPs (particularly smaller ones) may not necessarily have the resources to maintain a fully functioning and effective internal audit unit. In such cases, those DNFBPs should ensure that they take adequate measures to obtain the necessary capabilities from qualified external sources. They should also ensure that they have in place adequate internal capabilities to provide sufficient coordination with and oversight of any external resources they may utilize and that such external resources are adequately regulated and supervised by relevant Competent Authorities. When selecting external auditors, DNFBPs should take into consideration the potential candidate's cognizance of and ability to assess AML/CFT requirements as part of the selection process.

Some of the factors that DNFBPs should consider in determining the extent of audit testing of their AML/CFT Program by their independent audit functions include but are not limited to:

- The results of the NRA and other sectoral risk assessments;
- The nature, size, complexity, and geographic scope of the DNFBPs' business, and the results of their business-level ML/TF risk assessments;
- The risk profile associated with the products and services they offer and the markets and customers they serve;
- The frequency of supervision and inspection, and the nature of the feedback (including the imposition of administrative sanctions) they receive from the Banking Commissioner, as their AML/CFT supervisory authority, relative to enhancing the effectiveness of their AML/CFT measures;
- Internal and external developments concerning ML/FT risks, as well as developments in the management and operations of the DNFBPs.

The scope of such audits should include but not be limited to:

- Examining the adequacy of the DNFBP's ML/TF risk assessment framework and the application of a risk-based approach;
- Reviewing the adequacy of the DNFBP's AML/CFT Program, and whether it complies with regulatory requirements;
- Reviewing the effectiveness of the DNFBP's compliance function, including where CDD has been outsourced to third parties, such as the qualifications of the personnel, the contract, and the performance and reputation of the third party;

- Reviewing the effectiveness of DNFBP's staff in implementing and complying with the established internal policies, procedures, and controls;
- Assessing the training adequacy, including its comprehensiveness, accuracy of materials, training schedule, attendance tracking, and escalation procedures for lack of attendance.
- Reviewing case management and effectiveness of the suspicious activity reporting (SARs) mechanisms and systems, including a review of the criteria and processes for identifying and reporting suspicious transactions, an evaluation of the research and referral of unusual transactions, and a review of policies, procedures, and processes for referring unusual or suspicious activity from all business lines to the personnel responsible for investigating unusual activity. It shall also include reviewing internal suspicious transactions that have not been reported to the Banking Commissioner to determine the adequacy, completeness, and effectiveness of the SAT filing process.

5.10 AML/CFT Training

Section 2A.5 of the AML Regulations 2002 requires that the DNFBPs

"*must establish ongoing employee training to ensure that employees are trained on current money laundering, terrorist financing and proliferation financing techniques, methods, trends and indicators. Training must include a clear explanation of all aspects of money laundering/ terrorist financing/proliferation financing laws and obligations in the Marshall Islands, and in particular, the money laundering offence and penalties as they pertain to [the DNFBP] staff; CDD, and Suspicious Activity Reporting and the penalties that may apply to individual staff and officers for offences under the Banking Act.*"

DNFBPs must ensure that all their employees, officers, directors, and agents are aware of the risks of ML and TF relevant to the business, the applicable AML/CFT legislation, and their obligations and responsibilities under the legislation.

DNFBPs must provide appropriate and sufficient training, which is tailored to the nature, scale, and complexity of their business and which is proportionate to the level of ML/TF risk faced by the DNFBP.

DNFBPs must ensure that all employees, officers, directors, and agents:

- are made aware of the DNFBP's business-level risk assessment and how it affects their daily work;
- are trained concerning the DNFBP's AML/CFT policy, which should be drafted in unambiguous language;
- are trained in the DNFBP's procedures so that they can recognize and address potential instances of ML/TF;
- are made aware of the DNFBP's internal reporting procedures in respect of SARs and the identity and responsibilities of the DNFBP's compliance officer; and
- Understand their obligations under the Banking Act 1987 and AML Regulations 2002, as well as those of the DNFBP.

5.10.1 Role Specific and Tailored Training

DNFBPs should provide AML/CFT training that is specific to the role carried out by the member of staff. For example, front-line staff who interact with customers and perform transactions and services should be provided with AML/CFT training relevant to the performance of that role.

DNFBPs should also provide enhanced AML/CFT training tailored to the specific needs of staff who perform key AML/CFT roles within the DNFBP, for example, the Compliance Officer or Member of the Senior Management responsible for AML/CFT oversight.

DNFBPs must provide staff with ongoing training, especially where a staff member changes the role and they may encounter different ML/TF risks to that of their previous role.

5.10.2 Frequency of Training

DNFBPs should ensure that AML/CFT training is provided to all new employees upon joining the DNFBP promptly and to all staff at least on an annual basis thereafter.

Staff in customer-facing roles, with responsibilities relating to AML/CFT procedures or controls, should receive AML/CFT training before interacting with customers.

DNFBPs should consider the outcomes of their business-level risk assessments and whether the frequency and content of AML/CFT training provided are adequate for the levels of ML/TF risks faced by the business.

DNFBPs exposed to a higher level of ML/TF risk or who have greater exposure to constantly evolving ML/TF risks should provide training at more frequent and regular intervals.

5.10.3 Training Governance

DNFBPs should ensure senior management's oversight and responsibility for:

- the DNFBP's compliance with its requirements in respect of staff's AML/CFT training under the AML Regulations 2002;
- the establishment and maintenance of effective training arrangements which reflect the DNFBP's risk-based approach to AML/CFT; and
- ensuring that training content is reviewed and updated regularly to ensure that it remains relevant to the DNFBP and providing assurance to this effect.

5.10.4 Training of Outsource Service Providers

Where DNFBPs have outsourced an AML/CFT function, they should ensure that all staff at the outsource service provider performing AML/CFT activities on behalf of the DNFBP have been appropriately trained on:

- the ML/TF risks relevant to the DNFBP;
- the applicable AML/CFT legislation; and
- their obligations and responsibilities under the applicable AML/CFT legislation.

DNFBPs should ensure that the relevant staff in the outsourced entity are aware of the DNFBP's internal reporting procedures in respect of SARs and the identity and responsibilities of the DNFBP's Compliance Officer.

5.10.5 Training Channels

DNFBPs should decide the most appropriate method or methods they wish to use to provide AML/CFT training to staff, senior management, and agents. For example, DNFBPs may decide to use several different channels such as online or e-learning modules, classroom training, or video presentations to fulfill their obligations under the AML Regulations 2002.

5.10.6 Training Records

DNFBPs should keep a comprehensive record of:

- all staff, senior management, and agents who have received AML/CFT training;

- the type and content of AML/CFT training provided;
- the date on which the AML/CFT training was provided;
- the results of any testing carried out to measure employee's understanding of the AML/CFT requirements; and
- An ongoing training plan.

5.10.7 Management Information on Training

DNFBPs should ensure that the designated member of senior management is provided with timely AML/CFT management information including information on training and training completion.

DNFBPs should ensure that the senior management takes appropriate remediation action where there are concerns about training issues. Metrics concerning the DNFBP's training should be circulated to relevant senior management for management information purposes.

6. Customer Due Diligence (CDD)

6.1 Risk-based Application of CDD Measures

Sections 3A to 3L of the AML Regulations 2002 provides the CDD measures, which a DNFBP must take in order to comply with its obligations in respect of identifying and verifying customers, persons purporting to act on behalf customers and beneficial owners.

The level of CDD measures which a DNFBP is required to apply under Sections 3A to 3L of the AML Regulations 2002 depends upon the nature of the relationship between the DNFBP and its customer, the type of business conducted and the perceived ML/TF risks arising.

Section 3A.2 of the AML Regulations 200 specifically states that "*CDD must be applied on risk basis, which must include enhanced CDD for high-risk customers and politically exposed persons and may include simplified CDD for lower-risk customers.*"

CDD is the collective term for checks that DNFBPs are required to undertake on their customers, which may differ depending on the circumstances. It is holistic and is wider than simply undertaking identification and verification of customers or customers' beneficial owners.

Under the AML Regulations 2002, DNFBPs are obliged to apply a risk-based approach to CDD measures to mitigate the ML/TF risks identified in their business and customer risk assessment. The risk assessment framework of a DNFBP must identify which customers or categories of customers present higher risks and therefore require the application of enhanced CDD measures. Similarly, for customers who have been identified and categorized as presenting lower-risk, simplified CDD should be applied.

DNDBPs should however bear in mind that the application of a risk-based approach to CDD measures is not to be taken as a static formula i.e., always subjecting medium-risk customers to normal CDD measures and lower-risk customers to simplified CDD measures. Each customer's ML/TF risk profile is dynamic and subject to change depending on numerous factors, including (but not limited to) the discovery of new information or a change of behavior or activity. The appropriate level of CDD measures applicable to a customer should thus be adjusted according to the specific situation and risk indicators identified. The amount, type, and level of CDD undertaken should reflect and mitigate the nature of particular risks inherent in each customer, transaction, or matter.

DNFBPs must be able to demonstrate to the Banking Commissioner, as their supervisory authority, that the CDD measures they have applied are appropriate in mitigating the identified risks, by recording their reasoning and actions in this regard.

6.1.1 Assessing Customer and Business Relationship Risk

A customer of a DNFBP can be anyone who performs a one-off or occasional activity or transaction with a DNFBP, or anyone who establishes an ongoing commercial or business relationship with a DNFBP.

Assessing customer and business relationship risk is essential to the risk classification of customers as low, medium, or higher risk customers and for the effective application of appropriate risk-based CDD measures. DNFBPs should ensure that their customer and business relationship risk assessment processes are robust and reliable and that they incorporate the results of the NRA, any sectoral or thematic risk assessment, and their business-level ML/TF risk assessment, as the input of the relevant internal and external stakeholders, including the Compliance Officer and the Banking Commission.

When assessing customer and business relationship risk, DNFBPs should analyze customers based on identified risk factors to arrive at a risk classification. Fundamental to any assessment of customer risk is an assessment of whether the customer's financial circumstances, main business activities and source of wealth, and source of funds align with the background and wider profile of the customer. DNFBPs should detail these considerations in their customer and business relations risk assessments.

Some of the other considerations and factors that are relevant to customer and business relationship risk assessments and which should be considered by DNFBPs include but are not limited to:

- the structure, complexity, or nature of the customer entity or relationship makes it difficult to identify the true beneficial owner or any controlling interests;
- the customer appears to be attempting to obscure understanding of their business, ownership, or the nature of their matters;
- the customer is a PEP, or is closely related to or associated with a PEP;
- the instruction from the customer is channeled through a third party and there is a lack of direct interaction with the customer;
- there are any geographic risks associated with the customer; and
- the customer wishes to conduct the business relationship or request services in unusual circumstances.

Depending upon the nature and size of the DNFBPs' business, different methodologies can be used to accomplish the risk classification of customers. For example, entities with smaller or less complex businesses, may assess and assign customer risk classifications based on generic profiles for customers of the same type. On the other hand, large or more complex DNFBPs, may assess and assign customer risk classifications using more sophisticated models or scorecards based on the weightings of various risk factors.

Regardless of the methodologies chosen, DNFBPs should ensure that their customer and business relationship risk assessment processes and the rationale for their methodologies are well-documented, approved by senior management, and communicated at the appropriate levels of the organization. They should also decide on policies and procedures related to both the periodic review of their customer and business relationship risk assessment processes, and to the frequency of updating the individual business relationship risk assessments and customer risk classifications produced by them, taking into consideration changes in internal or external factors.

6.1.2 Establishing a Customer Risk Profile

Section 3B.3 of the AML Regulations 2002 requires that the DNFBPs "*must create a profile for each customer of sufficient detail to enable it to implement the CDD requirements of these Regulations. The customer profile should be based upon sufficient knowledge of the customer, including the customer's business with the [DNFBP] and the source of the customer's funds, wealth and/or assets.*"

DNFBPs must establish a risk profile for their customers, commensurate with the types and levels of risk involved. The customer risk profile should be based on DNFBP's sufficient knowledge of the customer, including the customer's business with the DNFBP and its source of wealth, funds, and/or assets. Such risk profiles allow DNFBPs to compare a customer's actual activity with the expected activity more effectively, and thus contribute to their capacity to discover unusual circumstances or potentially suspicious transactions.

In the case of DNFBP's customers that are legal persons or legal arrangements, the customer risk profile should include a detailed explanation or a structure chart providing details of beneficial owners, as defined under the AML Regulations 2002, of a legal person or a legal arrangement, and identifying the natural persons who ultimately own or control them. In addition, the risk profile of a legal person or legal arrangement should also Include a detailed explanation or a structure chart showing their internal management structure, identifying the persons holding senior management positions, or other positions of control. DNFBPs should also obtain information about the legal person's or arrangement's majority-owned or controlled operating subsidiaries, including the nature of the business and the operating locations of those subsidiaries.

To establish a customer risk profile, DNFBP's must also understand and obtain information on the intended purpose and nature of the business relationship (see 6.2.4 of these Guidelines). Depending on the type of customer, this information includes, but is not limited to:

- Information concerning the customer's or beneficial owner's business or occupation/employment;
- Information on the types of l products or services which the customer is looking for;
- Establishing the source of funds concerning the customer's anticipated pattern of transactions;
- Establishing the source of wealth of the customer (particularly for high-risk customers);
- Copies of the customer's most recent financial statements;
- Establishing any relationships between signatories and customers;
- Any relevant information of related third parties and their relationships with/to an account, for example, beneficiaries; or
- The anticipated level and nature of the activity that is to be undertaken through the business relationship, may include the number, size, and frequency of transactions that are likely to pass through the DNFBP's account.

Based on the risk profile, DNFBPs should accordingly carry out ongoing due diligence of their business relationships, to be able to ensure that the transactions or dealings conducted are consistent with the information they have about the customer, the type of activity they are engaged in, the risks they entail, and, where necessary, their source of funds.

6.1.3 New Customer Acceptance Policy

Section 3A.1 of the AML Regulations 2002 provides for the application of acceptance policies by DNFBPs to new customers.

DNFBPs should develop clear customer acceptance policies and procedures, including a description of the types of customers that are likely to pose a higher risk to a DNFBP.

In preparing such policies, the DNFBPs should state the factors that should be taken into consideration by the staff, which include but are not limited to:

- information on customer's background – business, industry, or profession;
- nature and intended purpose of the business relationship;
- country of origin, to determine whether those countries have adequate systems in place against money laundering and the financing of terrorism;
- determining the source of wealth and source of funds; and
- public or high-profile position.

Customer acceptance policies and procedures should accordingly be graduated and require more extensive due diligence for higher-risk customers, such as individuals planning to maintain a large account balance and conduct regular cross-border wire transfers or PEPs.

Decisions to enter into or pursue business relationships with higher-risk customers shall require the application of enhanced due diligence measures, such as approval to enter into or continue such business relationships being taken from the senior management. The customer acceptance policy should also define circumstances under which the DNFBP would not accept a new business relationship or would terminate an existing one, and if any suspicion has been raised, how to escalate the matter to the Compliance Officer.

6.2 Circumstances and Timing for Undertaking CDD Measures

In accordance with Section 3B.3 of the AML Regulations 2002, DNFBPs are required to identify and verify customers and where applicable, beneficial owners(s) at any time when:

- a person applies for a business relationship;
- a person seeks to engage in a threshold occasional transactions;
- a person seeks to carry a transfer of funds or value;
- a person engages in a suspicious activity; or
- where doubts have arisen as to the veracity or adequacy of previously obtained identification data on the person.

Under normal circumstances, DNFBPs are obliged to undertake CDD measures (including verifying the identity of customers, beneficial owners, beneficiaries, controlling persons, and authorized persons and understanding the nature of their business and the purpose of the business relationship) either before or during the establishment of a Business Relationship, or before the execution of a transaction for a customer with whom there is no Business Relationship, or before carrying out a transfer of funds or value.

Where doubts exist about a customer engaging in suspicious activity or about the veracity or adequacy of previously obtained customer identification information, the DNFBPs shall identify and verify the identity of the customer and beneficial owner before the customer may conduct any further business.

In determining when to take CDD measures with existing customers, some of the factors that DNFBPs should take into consideration include but are not limited to:

- any indication that the identity of the customer or customer's beneficial owner has changed;
- any transactions which are not reasonably consistent with his knowledge of the customer;
- any change in the purpose or intended nature of his relationship with the customer;
- any other matter which might affect the DNFBP's assessment of the money laundering or terrorist financing risk concerning the customer.

6.2.1 Establishment of a Business Relationship

DNFBPs establish a business relationship with a customer when they perform any act for, on behalf of, or at the direction or request of the customer, with the anticipation that it will be of an ongoing or recurring nature, whether permanent or temporary.

A business relationship will have "an element of duration".

There may be several indicators that a customer is establishing a business relationship, as opposed to the matter being an "occasional transaction" which includes but is not limited to:

- an explicit expectation from the customer or the DNFBP that a business relationship is being established;
- the nature of the customer or the transaction suggests they may wish to undertake more than one transaction e.g., it is in the nature of their business; or
- the transaction itself will inherently take time to complete e.g., the buying/selling of real estate.

6.2.2 Occasional Transactions

During their businesses, DNFBPs may perform occasional or non-recurring transactions for customers with whom there is no ongoing account or business relationship.

An occasional transaction is a transaction that falls outside of a "business relationship" i.e., where the customer-DNFBP relationship lacks an expectation of an "element of duration". To qualify as an occasional transaction, the relationship must be limited to a single service provided at a certain point in time.

When carrying out an occasional transaction that exceeds the total value of $10,000, either as a single transaction or a series of transactions that are linked, DNFBPs are required to identify the customer and verify the customer's identity as well as that of the beneficial owners, beneficiaries, controlling persons and authorized persons. DNFBPs should undertake appropriate risk-based CDD measures, including among other things understanding the nature of the customer's business and the intended purpose of the transaction, when carrying out an occasional transaction for a customer that exceeds the total value of $10,000, either as a single transaction or a series of transactions that are linked or when there is a suspicion of ML/TF.

6.2.3 Delayed Verification

Section 3D.1 of the AML Regulations 2002 allows a DNFBP to delay the verification of the identity of a customer under section 3B.3a., 3B.3b. and 3C for until after the establishment of the business relationship provided the DNDBP applies to and granted permission for delayed verification by the Banking Commissioner. However, as per section 3D.2 of the AML Regulations 2002, a DNFBP can only delay a verification in the following circumstances:

- where the delay is essential not to interrupt the normal course of business, and
- the risks of ML and TF are effectively managed.

In the above circumstances of delayed verification, DNFBPs are still required to carry verification as soon afterwards as reasonably practical.

While delayed verification is possible if permitted by the Banking Commissioner, Section 3D.3 nevertheless requires the DNFBPs to adopt certain risk management procedures establishing the conditions under which a customer may utilise the business relationship prior to verification. These include a set of measures, such as:

- limitation on the number, types and/or amount of transaction that can be performed; and
- enhanced monitoring of large and complex transactions being carried outside of the expected pattern for that relationship.

When DNFBPs avail of the provision of Section 3D of the AML Regulations 2002 for delayed verification, they should document and retain their reasons for doing so. In such circumstances, the verification of the identity must be conducted as soon as practical, and DNFBPs must ensure that they implement appropriate and effective measures to manage and mitigate the risks of money laundering and terrorist financing, and the customer benefits from the business relationship before the completion of the verification process.

Where DNFBPs are unable to take reasonable steps to verify the identity of the customer or beneficial owner, DNFBPs should be aware of their obligations under Section 3A.4 and Section 3J of the AML Regulations 2002 in this regard.

Section 3A.4 of the AML Regulations 2002 prohibits DNFBPs that are unable to identify and verify a customer and its beneficial owner or for whom sufficient information to form a customer profile cannot be gathered, from providing any service or carrying out any transactions sought by that customer. Section 34.A of the AML Regulations 2002 provides that DNFBPs must terminate any existing business relationship with the customer in such circumstances.

Section 3J of the AML Regulations 2002 provides that "*If the [DNFBP]has already commenced a business relationship and is unable to comply with the CDD required for a customer, or where CDD identifies an unlawful, or unexplained, source for the customer's funds and wealth it must terminate the customer relationship and file a suspicious activity report under Section 5*."

6.3 CDD Measures

The application of risk-based CDD measures is comprised of several components, in keeping with the customer's ML/FT risk classification and the specific risk indicators that are identified. Generally, these components include, but are not limited to, the following categories:

- Identification of the customer, beneficial owners, beneficiaries, controlling persons, and authorized persons; and the verification of their identity based on documents, data, or information from reliable and independent sources (see 6.3.1 of these Guidelines);
- Screening of the customer, beneficial owners, beneficiaries, controlling persons, and authorized persons to screen for the applicability of targeted or other international financial sanctions, and particularly in higher-risk situations, to identify any potentially adverse information (see 6.4 of these Guidelines);
- Understanding and obtaining information on the nature and intended purpose of the business relationship, and in the case of legal persons and legal arrangements, understanding the nature of the customer's business and the ownership and control structure of the customer, including the ultimate natural person(s) who owns or controls a legal person including natural persons with a controlling interest (see 6.3.2 and 6.3.1.5 of these Guidelines);
- Ongoing monitoring of the business relationship to ensure consistency between the transactions or activities conducted and the information that has been gathered about the customer and their expected behavior (see 6.3.3 of these Guidelines);
- Scrutinizing transactions undertaken throughout that relationship to ensure that the transactions being conducted are consistent with the DNFBP's knowledge of the customer, their business, and risk profile, including where necessary, the source of funds.
- Ensuring that documents, data, or information collected under the CDD process is kept up to date and relevant, by undertaking reviews of existing records, particularly for higher-risk customers and PEPs.

In cases involving higher levels of risk, DNFBPs are generally required to apply enhanced CDD measures, such as identifying and/or verifying the customer's source of funds and source of wealth and taking other appropriate risk-mitigation measures (see 6.4 of these Guidelines).

As a part of their AML/CFT Program, DFBPs must take a risk-based approach in developing the internal CDD policies, procedures, and controls.

6.3.1 Customer and Customer's Beneficial Owners' Identification and Verification

The identification and verification of the identity of customers is a fundamental component of an effective ML/TF risk management and mitigation program. DNFBPs are obliged to identify customers, including beneficial owners, beneficiaries, controlling persons, and authorized persons, whether a natural or legal person or legal arrangement, and to verify their identity using documents, data, or information obtained from reliable and independent sources.

The specific requirements concerning the timing, extent and methods to identify and verify the identity of customers and beneficial owners depend in part on the type of customer (whether a natural or legal person) and on the level of risk involved (also see 6.4 Enhanced CDD Measures, and 6.5 Simplified CDD Measures). Thus, the type and nature of the customer (including beneficial owners, beneficiaries, controlling persons, and authorized persons) should be considered as risk factors in determining the type of CDD that should be applied, whether standard CDD, Enhanced CDD, or Simplified CDD.

DNFBPs must use a risk-based approach to determine the internal policies, procedures, and controls they implement concerning the identification and verification of customers (including beneficial owners, beneficiaries, controlling persons, and authorities. They should however be reasonable and proportionate to the risks involved, and in formulating them, DNFBPs should incorporate the procedures provided under Schedule 1 of the AML Regulations 2002.

6.3.1.1 CDD measures for customers who are natural persons

Schedule 1 of the AML Regulations provides that the DNFBPs are required to obtain the following information to identify and verify the identity of a customer who is a natural person:

(a) full and correct name of person and any other names previously held;
(b) permanent address;
(c) telephone (not including mobile phone number) and fax number (if any);
(d) date and place of birth;
(e) nationalities and citizenships held currently and previously by the applicant;
(f) occupation and name of employer (if self employed, the nature of the self employment);
(g) copy of first two pages of passport or copy of national identity card showing the following details:
    i. number and country of issuance;
    ii. issue and expiry date;
    iii. signature of the person (applicable only to national identity card);
(h) signature;
(i) purpose of the account and the potential account activity;
(j) written authority to obtain independent verification of any information provided;
(k) source of income or wealth;
(l) written confirmation that all credits to the account are and will be beneficially owned by the [account] holder;
(m) any documentary or other evidence reasonably capable of establishing the identity of that person.

The above information requirements also apply to identify and verify the identity of beneficial owners and controlling persons.

The verification of a customer's identity, including their address, should be based on original, official (i.e. government-issued) documents whenever possible. When that is not possible, DNFBPs should augment the number of verifying documents or the amount of information they obtain from different independent sources. They should also identify the lack of official documents and the use of alternative means of verification as risk factors when assessing the customer's ML/FT risk classification.

The types of address verification that may generally be considered acceptable include, but are not limited to, the following categories of documents issued in the name of the customer:

- Bills or account statements from public utilities, including electricity, water, gas, or telephone line providers;

- Local and national government-issued documents, including national identity cards or municipal tax records;
- Registered property purchase, lease, or rental agreements;
- Documents from supervised third-party financial institutions, such as bank statements, credit or debit card statements, or insurance policies.

6.3.1.2 CDD measures for Beneficial Owners

DNFBPs should note that there is an obligation to identify all beneficial owners. In addition, DNFBPs are required to take reasonable steps to verify the identity of beneficial owners by using relevant documents, data, or information obtained from a reliable and independent source.

Schedule 1A. of the AML Regulations 2002 provides the information that a DNFBP is required to obtain to identify and verify the identity of beneficial owners. However, DNFBPs should verify the identity of beneficial owners by taking those measures reasonably warranted by a risk-based approach following an assessment of the ML/TF risks presented by the customer. In complying with their obligations to identify and verify the identity of a customer's beneficial owner(s), and in circumstances where a senior managing official(s) has been listed as a customer's beneficial owner(s), DNFBPs should establish whether their customer has exhausted all possible means to identify their beneficial owner(s).

In this regard, DNFBPs should:

- Compile documented assessments determining scenarios where beneficial ownership may be a factor concerning the provision of products and services offered by the DNFBP; and
- Assess and document:
    - the degree of verification required regarding the beneficial owners depending on the associated ML/TF risk attached to such beneficial owners;
    - the procedures to be applied in these circumstances; and
    - where relevant, measures taken to identify a beneficial owner, and any difficulties encountered in establishing a beneficial owner's identity.

6.3.1.3 CDD measures for Beneficiaries

In addition to the CDD measures required for the customer and beneficial owners, DNFBPs are also required to identify and verify the identity of the beneficiary or beneficiaries for life and other investment-linked insurance.

Section 3C.2 of the AML Regulations 2002 provides that "*as soon as the beneficiary [of a life and other investment-linked insurance policy] is identified or designated, the [DNFBP] must:*

a. take the name of any beneficiary identified as a specifically named natural or legal person or arrangement; and
b. obtain sufficient information concerning any beneficiary designated by characteristics, class, or other means to satisfy itself that it will be able to establish the beneficiary's identity at the time of the payout."

Schedule 1 of the AML Regulations 2002 provides the information that a DNFBP is required to obtain to identify and verify the identity of authorized persons who are natural persons, legal persons, and legal arrangements.

6.3.1.4 CDD measures for Authorised Persons

In addition to identifying and verifying the identity of customers, beneficial owners, beneficiaries, and controlling persons, DNFBPs must verify the identity of any person authorized to act or transact business on behalf of the customer, whether the customer is a legal or natural person. Such persons may include but are not limited to:

- Signatories or other authorized persons in case they are authorized to act on behalf of the customer;
- Parents or legal guardians of a minor child, or legal guardians of a physically or mentally disabled or incapacitated person;
- Attorneys or other legal representatives.

Schedule 1 of the AML Regulations 2002 provides the information that a DNFBP is required to obtain to identify and verify the identity of authorized persons who are natural persons, legal persons, or legal arrangements.

When verifying that a person purporting to act on behalf of a customer is so authorized, the following types of documents may generally be considered to be acceptable:

- A legally valid power of attorney;
- A properly executed resolution of a legal person's or legal arrangement's governing board or committee;
- A document from an official registry or other official sources, evidencing ownership or the person's status as an authorized legal representative;
- A court order or other official decision.

6.3.1.5 CDD Measures concerning Legal Persons and Legal Arrangements

DNFBPs are obliged to undertake CDD measures concerning legal persons and legal arrangements, including identification and verification of the identity of the beneficial owners, beneficiaries, and other controlling persons, in accordance with the provisions of the AML Regulations 2002.

DNFBPs should incorporate the procedures provided under Schedule 1 of the AML Regulations 2002 in their internal policies, procedures, and controls on the information required to be obtained to identify and verify the identity of legal persons and legal arrangements.

In addition, for customers that are legal persons and legal arrangements, DNFBPs are required to understand the nature of the customer's business and the ownership and control structure of the customer, including the ultimate natural person(s) who owns or controls a legal person or legal arrangement, including the natural person with a controlling interest.

Where a customer is a legal person, DNFBPs must identify and take reasonable measures to verify the identity of beneficial owners by obtaining information on –

a. the identity of all the natural persons who own directly or indirectly 25% or more of the vote or value of an equity interest in the legal person;
b. where there is doubt under paragraph (a) above as to whether the person identified is/are the beneficial owner (s) or where no natural person exerts control through ownership interests, the identity of the natural person exercising control of the legal person through other means, as may be specified by the Banking Commissioner, including through the chain of corporate vehicles and through formal or informal nominee arrangements; and
c. where no natural person is identified under paragraphs (a) and (b), the identity of the natural person who holds the position of senior managing official.

For customers that are legal arrangements, DNFBPs must identify and take reasonable measures to verify the identity of beneficial owners by obtaining information:

a. for trusts, on the identity of the settlor(s), the trustee(s), protector (if any), all the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust, including through a chain of control or ownership;
b. for other types of legal arrangements, on the identity of persons in equivalent or similar positions.

For beneficiaries of trusts or other legal arrangements that are designated by characteristics or by class, the DNFBP must obtain sufficient information concerning the beneficiary to satisfy the DNFBP that it will be able to establish the identity of the beneficiary at the time of the pay-out or when the beneficiary intends to exercise vested rights.

6.3.2 Purpose and Nature of the Business Relationship

DNFBPs should identify the most appropriate information necessary to satisfy their obligations under Section 3B.7 of the AML Regulations 2002. Depending on the type of customer, the information might include, for example:

- Information concerning the customer's or beneficial owner's business or occupation/employment;
- Information on the types of financial products or services which the customer is looking for;
- Establishing the source of funds in relation to the customer's anticipated pattern of transactions;
- Establishing the source of wealth of the customer (particularly for high-risk customers);
- Copies of the customer's most recent financial statements;
- Establishing any relationships between signatories and customers;
- Any relevant information on related third parties and their relationships with/to an account, for example, beneficiaries; or
- The anticipated level and nature of the activity that is to be undertaken through the business relationship, may include the number, size, and frequency of transactions that are likely to pass through the DNFBP's account.

While DNFBPs are obliged under 3B.7 of the AML Regulations 2002 to obtain information on the purpose and intended nature of the business relationship at the outset of the relationship, the reliability of this profile should increase over time as the DNFBP learns more about the customer, their use of products/accounts and the services that they require. DNFBPs should ensure they review any known information on the customer and monitor their transactions/activity, to ensure they understand the potentially changing purpose and nature of the business relationship.

6.3.3 Ongoing Monitoring of the Business Relationship

Section 3I.1 of the AML Regulations 2002 requires the DNFBPs to conduct ongoing monitoring of business relationships, which must include "*the scrutiny of customer transactions to ensure that they are being conducted according to the [DNFBP's] knowledge of the customer and the customer's business and risk profile, the source of funds, and may include pre-determined limits on amount of transactions and types of transactions.*"

DNFBPs must ensure that they have effective and appropriate ongoing monitoring policies and procedures that are in place, in operation, and adhered to by all staff concerning monitoring of customers' transactions and activities, as well as in regard to the extent of monitoring for specific customers or categories of customers. Such policies and procedures should include at a minimum:

- Full review and consideration of all trigger events associated with their customers. Clear examples of trigger events that are understood by staff and targeted training should be provided for staff on how to identify possible trigger events and interpret these. Trigger events should also be reviewed regularly by the DNFBPs and examples revised where appropriate;
- A well-documented and well-established monitoring program, which is demonstrative of a risk-based approach, where high-risk customers are reviewed frequently;
- Periodic reviews of customers, the frequency of which is commensurate with the level of ML/TF risk posed by the customer. DNFBPs should also ensure that staff are provided with specific training on how to undertake a periodic review;
- Reassessment and, if applicable, re-categorization of customers upon material updates to CDD information and/or other records gathered through a trigger event or periodic review;
- Re-categorisation of customers as high risk subject to senior management approval and the completion of Enhanced Due Diligence before a decision is taken to continue the relationship;
- Screening was undertaken on all customers to identify new and ongoing PEP relationships. The frequency of such screening should be determined by the DNFBP, commensurate with the DNFBP's Business-level risk assessment;
- Clear instruction for staff regarding the action required where appropriate CDD documentation or information is not held on file. Such instruction should include the steps that may be taken to locate or obtain such documentation or information; and
- Proactive utilization of customer contact as an opportunity to update CDD information.

Some of the methods that DNFBPs may employ for the ongoing monitoring of transactions include, but are not limited to:

- Threshold-based rules, in which transactions above certain pre-determined values, numerical volumes, or aggregate amounts are examined;
- Transaction-based rules, in which the transactions of a certain type are examined;
- Location-based rules, in which the transactions involving a specific location (either as origin or destination) are examined;
- Customer-based rules, in which the transactions of particular customers are examined.

DNFBPs may use all or any combination of the above methods, or any others that are appropriate to their particular circumstances, for effective ongoing monitoring of the business relationship and customer transactions. Furthermore, monitoring systems and methods may be automated, semi-automated, or manual, depending on the nature and size of their businesses.

6.3.3.1. Monitoring Complex Transactions

Section 3I.2 of the AML Regulations 2002 provides that DNFBPs "*must pay special attention to all complex, unusual large transactions, or unusual pattern of transactions that have no visible economic or lawful purpose. [DNFBPs] must examine as far as possible the background and purpose of such transactions and set forth their findings in writing.*"

As discussed in Sections 6.3.3 of these Guidelines, DNFBPs are required to monitor customer transactions to identify transactions that may be suspicious, and the intensity of the monitoring should

increase with the complexity and scale of those transactions so that the risk of ML/TF is factored into the transaction monitoring process.

In the case of complex, unusual large transactions, or unusual patterns of transactions that have no visible economic or lawful purpose, DNFBPs are expected to investigate and obtain more information about the background and purpose of transactions, and to conduct enhanced ongoing monitoring and review of transactions to identify potentially unusual or suspicious activities.

6.3.4 Reviewing and Updating the CDD Information

Section 3H of the AML Regulations 2002 provides that the DNFBPs "*must gather and maintain customer information on an ongoing basis. Documents, data or information collected under the CDD process should be kept up to date and relevant by undertaking reviews of existing records at appropriate times, particularly for higher risk categories of customers or business relationships.*"

The timely review and update of CDD information is a fundamental component of an effective ML/FT Program. DNFBPs are obliged to maintain the CDD documents, data, and information obtained on customers, including their beneficial owners, beneficiaries, controlling persons, and authorized persons up to date. DNFBPs should update the CDD information on higher-risk categories of customers or business relationships more frequently.

To be able to update the CDD information of customers in a risk-based manner, DNFBPs should develop internal policies, procedures, and controls concerning the periodic or event-driven review and updating of CDD information. These policies and procedures should be reasonable and proportionate to the risks involved, and, in formulating them, some of the parameters that DNFBPs should take into consideration include, but are not limited to:

- Circumstances, timing, and frequency of reviews and updates

  Generally, DNFBPs should establish clear rules per customer risk category concerning the maximum period that should be allowed to elapse between CDD reviews and updates of customer records. The expiry of a customer's or beneficial owner's identification documents is a circumstance that calls for updating the customer information. Changes in legislation or internal procedures are also a cause for reviewing and updating customer files.

- Triggering circumstances or events for interim review

  In addition to the above, DNFBPs should also establish clear rules concerning circumstances or events that would trigger an interim review or the acceleration of a particular customer's review cycle. Circumstances or events that might trigger an interim review include:
  - Discovery of information about a customer that is either contradictory or otherwise puts in doubt the appropriateness of the customer's existing risk classification or the accuracy of previously gathered CDD information;
  - Material change in ownership, legal structure, or other relevant data (such as name, registered address, purpose, capital structure) of a legal person or arrangement;
  - Initiation of legal or judicial proceedings against a customer, including the beneficial owner(s), beneficiaries, controlling person(s), or authorized person(s);
  - Finding materially adverse information about a customer, including the beneficial owner(s), beneficiaries, controlling person(s), or authorized person(s), such as media reports about allegations or investigations of fraud, corruption, or other crimes;
  - Transactions that indicate potentially unusual or suspicious transactions or activities.

- Components and extent of reviews and updates

Depending upon the nature and size of the business, DNFBPs should clearly define the contents and extent of CDD reviews for business relationships in different risk categories, including which data elements, documents, or information should be examined and updated if necessary. In this regard, DNFBPs are advised that tools such as checklists and procedural manuals will help to enhance the effectiveness of CDD reviews and updates. Examples of procedures might include, but are not necessarily limited to:

- When the source of wealth or the source of funds of a customer should be verified;
- When additional inquiries or investigations should be made about the nature of a customer's business, the purpose of a business relationship, or the reasons for a transaction;
- How much of a customer's transactional history, including how many and which specific transactions or transaction types, should be reviewed as part of a periodic or an interim review.

6.4 Enhanced CDD Measures

In keeping with their risk-based approach to CDD, DNFBPs are obliged to apply enhanced CDD measures in those situations where they have determined that customers or business scenarios present a higher ML/TF risk.

Generally, enhanced CDD measures involve a more rigorous application of CDD measures, including elements such as:

- Increased scrutiny and higher standards of verification and documentation from reliable and independent sources concerning customer identity;
- More detailed inquiry and evaluation of reasonableness regarding the purpose of the business relationship, the nature of the customer's business, the customer's source of funds and source of wealth, and the purpose of individual transactions;
- Increased monitoring of the business relationship, including the requirement for senior management approval, more frequent monitoring of transactions, and more frequent review and updating of customer due diligence information.

When applying enhanced CDD measures to customers or business relationships, DNFBPs should ensure that they document their rationale. This includes, for example:

- DNFBPs should ascertain whether they have obtained adequate information regarding the customer and the customer's business in the context of the product or service they are providing to the customer, to form a basis for a reliable and comprehensive assessment of the risks arising.

  If the information is not adequate, DNFBPs should seek additional documentation, which may include, for example:
  - Establishing a customer's source of wealth/source of funds; and/or
  - Additional information regarding the customer and/or service, including additional CDD information in any case where the DNFBP has doubts about the veracity or adequacy of information previously obtained.

- DNFBPs should apply an enhanced level of ongoing monitoring to their business with the customer, as appropriate to their assessment of the ML/TF risk arising from the business with that customer. DNFBPs should review the level of that monitoring regularly to ensure that it remains risk-sensitive.

DNFBPs must apply enhanced CDD measures to higher-risk situations to manage and mitigate those risks appropriately. Appendix 1 Part B of the AML Regulations 2002 provides examples of higher-risk

situations in which enhanced CDD measures should be applied, which shall be referred to by DNFBPs in determining when enhanced CDD measures are appropriate.

DNFBPs should note that enhanced CDD measures cannot be substituted for CDD measures but must be applied in addition to CDD measures.

6.4.1 EDD requirements for Politically Exposed Persons (PEPs)

The PEP regime in RMI only includes foreign PEPs.

Section (a)(17) of the AML Regulations 2002 defines a PEP as "*any person who is or has been entrusted with a prominent public function in a foreign country including, but not limited to Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned companies, and important political party officials. Family members and close associates who have business relationships with such persons are also included herein.*"

PEPs can pose a higher money laundering risk to DNFBPs as their position may make them vulnerable to corruption. This risk, and therefore enhanced CDD requirements for PEPs, also extends to their family members and close associates.

DNFBPs should note that PEP status itself is intended to apply higher vigilance to certain individuals and put those individuals that are customers or beneficial owners into a higher risk category. It is not intended to suggest that such individuals are involved in suspicious activity.

In demonstrating compliance with the obligations set out under Section 3K of the AML Regulations 2002 relating to PEP customers, DNFBPs should undertake the measures outlined in Sections 6.4.1.1 to 6.4.1.4 below.

6.4.1.1 Policies and Procedures in relation to PEPs

A. PEP Identification

DNFBPs must put appropriate policies and procedures in place to determine:

- if a customer or beneficial owner is a PEP at boarding; or
- if a customer or beneficial owner becomes a PEP during the business relationship with the DNFBP.

DNFBPs should note that new and existing customers may not initially meet the definition of a PEP, but may subsequently become one during a business relationship with the DNFBP. On this basis, DNFBPs must undertake regular and ongoing screening of their customer base and the customers' beneficial owners (where relevant), to ensure that they have identified all PEPs. The frequency of PEP screening should be determined by DNFBPs commensurate with their business-level ML/TF risk assessment.

B. Management of PEPS

DNFBP's policies and procedures must address how any identified PEP relationships will be managed by the DNFBP including:

- Application of enhanced CDD measures to PEPs, including determining the source of wealth and source of funds;
- Obtaining senior management Approval; and
- Enhanced ongoing monitoring measures.

DNFBPs are required to develop and maintain a list of PEPs and other higher-risk customers.

C. Reliance on Third Parties in relation to PEPs

DNFBPs should also have appropriate policies and procedures in place in instances where they rely on third parties to perform their due diligence measures on customers and beneficial owners. The policies and procedures should set out the steps to be taken by the DNFBP when the third party has identified a new PEP relationship.

DNFBPs should not rely on third parties to perform enhanced CDD measures or to provide senior management approval. However, third parties may assist the DNFBP in gathering the necessary documentation or information to establish the source of wealth and source of funds.

D. Domestic and International organization PEPs

Although domestic and international organization PEPs are not included within the definition of 'PEPs' as provided under Section a(17) of the AML Regulations 2002 requiring the application of enhanced CDD measures from the beginning, DNFBPs are however required to have appropriate policies and procedures in place to identify domestic and international organization PEPs. In accordance with their ML/TF risk assessment framework, DNFBPs must determine the risk posed by the domestic and international organization PEPs and apply the CDD measures, including enhanced CDD measures, commensurate with the risk involved.

6.4.1.2 Senior Management Approval of PEPs

DNFBPs should put appropriate policies and procedures in place setting out:

- the reporting and escalation of PEP relationships to senior management (up to and including the Member of Senior Management (as defined in 5.4 of these Guidelines), where relevant and appropriate);
- The timelines for obtaining senior management sign-off; and
- The level of seniority required to approve a PEP relationship.

The DNFBP must allocate responsibility for the approval of PEP relationships and must ensure that the approval of a PEP relationship is conducted by individuals who are appropriately skilled and empowered, and this process is subject to appropriate oversight. DNFBPs should determine the level of seniority for sign-off by the level of increased ML/TF risk associated with the business relationship. The member of senior management approving a PEP business relationship should have sufficient seniority and oversight to make informed decisions on issues that directly impact the DNFBP's ML/TF risk profile.

When considering whether to approve a PEP relationship, DNFBPs should take into consideration;

- The level of ML/TF risk that the DNFBP would be exposed to if it entered into the business relationship with a PEP; and
- What resources the DNFBP would require to mitigate the risk effectively.

When DNFBPs are considering whether to enter into or to continue to carry on a business relationship with a PEP, they should ensure that:

- the matter is discussed at the senior management level;
- the corresponding ML/TF risks are acknowledged; and
- the decision reached is documented.

6.4.1.3 Source of Wealth/Source of Funds of PEPs

DNFBPs must take adequate measures to establish the source of wealth and source of funds, which are to be used in the business relationship to satisfy themselves that they do not handle the proceeds of corruption or other criminal activity.

The measures, that DNFBPS should take to establish a PEP's source of wealth and source of funds will depend on the degree of risk associated with the business relationship. DNFBPs must verify the source of wealth and the source of funds based on reliable and independent documents, data, or information.

When determining the source of wealth and source of funds, DNFBPs should at least consider:

- The activities that have generated the total net worth of the customer (that is, the activities that produced the customer's funds and property); and
- The origin and the means of transfer for funds that are involved in the transaction (for example, their occupation, business activities, proceeds of the sale, corporate dividends).

6.4.1.4 Enhanced ongoing monitoring of the business relationship with PEPs

DNFBs must regularly review the information they hold on PEP customers to ensure that any new or emerging information that could affect the risk assessment is identified in a timely fashion. This includes periodically obtaining independent, verified information on the source of funds, wealth, and assets, as well as a periodic examination of PEP transactions. The frequency of ongoing monitoring should be determined by the DNFBP commensurate with the higher risk associated with the PEP relationship.

6.4.2 Enhanced CDD measures for High-Risk Customers or Transactions

DNFBPs are obliged to apply enhanced CDD measures to manage and mitigate the risks associated with identified higher-risk customers and/or transactions. It necessarily means that the DNFBPs should intensify their CDD measures, specifically by obtaining further information and evidence from the higher-risk customer, which includes but is not limited to:

- Source of funds and source of wealth;
- Identifying information on individuals with control over the customer;
- Occupation or type of business;
- Financial statements;
- Banking references;
- Domicile;
- Description of customer's business activity, sector, or profession; the anticipated number of transactions, turnover, and list of customers and suppliers; and
- Any relationships with third parties or intermediaries.

When carrying out enhanced CDD measures, DNFBPs should pay particular attention to the reasonableness of the information obtained, and should evaluate it for possible inconsistencies and potentially unusual or suspicious circumstances.

DNFBPs are required to have proper risk management systems in place to identify higher-risk customers and must develop and maintain a list of such customers. They must have proper internal policies and procedures to seek senior management approval before accepting any higher-risk customer or continuing a relationship with a customer that subsequently became a higher-risk customer after the establishment of the business relationship.

DNFBPs must conduct enhanced ongoing monitoring of all their higher-risk customers. They must regularly review the information they hold on higher-risk customers to ensure that any new or

emerging information that could affect the risk assessment is identified in a timely fashion. This includes periodically obtaining independent, verified information on the source of funds, wealth, and assets, as well as a periodic examination of transactions of higher-risk customers. The frequency of ongoing monitoring should be determined by the DNFBP commensurate with the higher risk associated with the relationship with higher-risk customers.

6.4.3 Enhanced CDD requirements for Higher-Risk Countries

Under Section 10(d) of the AML Regulations 2002, DNFBPs are required to comply with the provisions of Section 3I.3 relating to higher-risk countries

Section 3I.3 of the AML Regulations 2002 provides that DNFBPs "*must pay special attention to all business relationships and transactions with legal persons, natural persons, and financial institutions from countries that are not sufficiently applying the FATF standards and recommendations. Enhanced due diligence should be proportionate to the level of risk involved, and follow the procedures presented in Section 3K [that relates to enhanced CDD for higher-risk customers and PEPs]* "

DNFBPs are obliged to implement enhanced CDD measures commensurate with the ML/FT risks associated with business relationships and transactions with customers from higher-risk countries i.e., the countries identified by FATF as not sufficiently applying its standards and recommendations and the countries identified by the Banking Commission. In the case of legal persons and arrangements, this also includes their beneficial owners, beneficiaries, and other controlling persons if they are from higher-risk countries.

DNFBPs could obtain guidance on higher-risk countries from the Banking Commissioner, from the FATF list of high-risk and other monitored jurisdictions, and the NRA report. In addition, reference could also be made to the Organisation for Economic Cooperation and Development (OECD) list of jurisdictions classified as tax havens. The Basel AML index can also be a useful source to determine the risk of a country.

Examples of some of the measures DNFBPs should apply in this regard include:

- Increased scrutiny and higher standards of verification and documentation from reliable and independent sources concerning the identity of customers, beneficial owners, beneficiaries, and other controlling or authorized persons;
- More detailed inquiry and evaluation of reasonableness regarding the purpose of the business relationship, the nature of the customer's business, the customer's source of funds, and the purpose of individual transactions;
- Increased investigation to ascertain whether the customers or related persons (beneficial owners, beneficiaries, and other controlling or authorized persons, in the case of legal persons and arrangements) are foreign PEPs;
- Increased supervision of the business relationship, including the requirement for higher levels of internal reporting and management approval, more frequent monitoring of transactions, and more frequent review/ updating of customer due diligence information.

To fulfill their obligations under the AML Regulations 2002, and commensurate with the nature and size of their businesses and the risks involved, DNFBPs should establish adequate internal policies, procedures, and controls concerning the application of enhanced CDD measures and risk-proportionate effective countermeasures to customers and business relationships associated with

high- risk countries. Some of the factors to which DNFBPs should give consideration when formulating such policies, procedures, and controls, include but are not limited to the following:

- the DNFBP's risk appetite concerning business relationships involving higher-risk countries;
- methodologies and procedures for assessing and categorizing country risk, and identifying higher-risk countries, including the statutorily defined higher-risk Countries as established by the Banking Commission, and taking into consideration advice or notifications of concerns about weaknesses in the AML/CFT system of other countries issued by the relevant Banking Commission and/or other competent authorities;
- determination and implementation of appropriate risk-based controls (for example, certain product or service restrictions, transaction limits, or others) concerning customers and business relationships associated with higher-risk countries;
- organizational roles and responsibilities concerning the monitoring, management reporting, and risk management of higher-risk country business relationships;
- appropriate procedures for the enhanced investigation of business relationships involving high-risk countries concerning their assessment for possible PEP associations;
- Independent audit policies in respect of enhanced CDD procedures about customers/business relationships involving higher-risk countries and the business units that deal with them.

For all countries identified as higher risk, the FATF calls on all members and urges all jurisdictions to apply Enhanced CDD measures, and in the most serious cases, countries are called upon to apply countermeasures to protect the international financial system from the ongoing money laundering, terrorist financing, and proliferation financing risks emanating from the country. However, specific countermeasures which need to be applied by DNFBPs shall be advised by the Banking Commission.

6.5 Simplified CDD Measures

Section 3A.2 of the AML Regulations 2002 requires the DNFBPs to apply CDD measures on a risk-sensitive basis, which means that they must apply enhanced CDD measures for higher risk customers and politically exposed persons and simplified CDD measures for lower-risk customers.

To apply simplified CDD measures to lower-risk customers, Section 3L.1 requires DNFBPs to apply and seek authorisation from the Banking Commissioner. The Banking Commissioner may grant authorisation only if:

- a lower risk has been identified;
- allowing simplified CDD measures is consistent with the Marshal Island's NRA;
- the DNFBP complies with Section 2 of the AML Regulations 2002 that relates to internal policies, procedures, controls and training;
- the DNFBP presents a simplified CDD procedure for the business relationship or transaction that complies with the other provisions of this section 3L.

Section 3L.2 of the AML Regulations 2002 further provides that under certain circumstances it would be reasonable to grant permission to DNFBPs to apply simplified CDD measures when identifying and verifying the identity of the customer or customer's beneficial owner, which includes

- when the risk of money laundering and terrorist financing is lower; or
- when information on the identity of the customer and customer's beneficial owner is publicly available; or
- where adequate checks and controls exist in national systems.

Under Section 3L.3 of the AML Regulations 2002 the application of simplified CDD measures on non-resident customers or customer's beneficial owners is only limited to countries that are in compliance with, and effectively implementing FATF Recommendations and are not included in the list of tax or money laundering havens.

Appendix 1 Part C of the AML Regulations 2002 provides examples of lower risk situations in which simplified CDD measures should be applied, which shall be referred to by DNFBPs in determining when simplified CDD measures are appropriate.

6.5.1. Simplified CDD measures that DNFBPs can apply to their business relationships or transactions

DNFBPs should identify the most appropriate simplified CDD measures to apply to business relationships or transactions following their internal policies and procedures. Simplified CDD measures, which DNFBPs may apply include, but are not limited to:

- Adjusting the timing of CDD where the product or transaction sought has features that limit its use for ML/TF purposes, for example by:
    - Verifying the customer's or beneficial owner's identity during the establishment of the business relationship; or
    - Setting defined thresholds, above or after which the identity of the customers or beneficial owners must be verified. In such circumstances, DNFBPs should make sure that:

  - This does not result in a *de facto* exemption from CDD;
  - They have systems or processes in place to detect when the threshold has been reached; and
  - They do not defer CDD or delay obtaining relevant information about the customer unless permission has been first granted by the Banking Commissioner.
- Adjusting the quantity of information obtained for identification, verification, or monitoring purposes; for example, by verifying identity based on information obtained from one reliable, credible and independent document or data source only.
- Adjusting the quality or source of information obtained for identification, verification, or monitoring purposes, for example by:
  - Accepting information obtained from the customer rather than an independent source when verifying the beneficial owner's identity (note that this is not permitted concerning the verification of the customer's identity);
  - Relying on the source of funds to meet some of the CDD requirements, where the risk associated with all aspects of the relationship is very low, for example where the funds are stated benefit payments;
- Adjusting the frequency of CDD updates and reviews of the business relationship, depending on the level of risk associated with that customer; or
- Adjusting the frequency and intensity of transaction monitoring, for example by monitoring transactions above a certain threshold only. Where DNFBPs choose to do this, they should ensure that the threshold is set at a reasonable level and that they have systems in place to identify linked transactions that, together, would exceed that threshold.

When applying simplified CDD measures, DNFBPs should obtain sufficient information to enable them to be reasonably satisfied that their assessment of the low ML/TF risk associated with the relationship is justified. DNFBPs should obtain sufficient information about the nature of the business relationship to identify any unusual or suspicious transactions. DNFBPs should note that simplified CDD measures do not exempt them from reporting suspicious transactions to the Banking Commissioner.

6.5.2. Public Companies

Section 3C.3 of the AML Regulations 2002 provides that

"*For public companies (or other legal persons or legal arrangements) quoted on an exchange regulated by the Banking Commission, and certain non-resident public companies subject to adequate regulatory disclosure requirements and quoted on a foreign exchange approved for this purpose by the Banking Commission that is subject to adequate supervision in a jurisdiction that is implementing effectively the FATF Recommendations, no further identification is necessary.*"

When the customer or customer's beneficial owner or controlling person is a public company listed on a regulated stock exchange, as approved by the Banking Commission, and is subject to adequate disclosure and transparency requirements related to beneficial ownership, DNFBPs are not required to obtain further information to identify and verify the identity of the beneficial owners of such public companies.

In the case of non-resident public companies that are listed on the foreign stock exchange, which is approved by the Banking Commission, DNFBPs should take steps to adequately assess and document the relevant disclosure and transparency requirements related to beneficial ownership. DNFBPs must

ensure that these foreign countries apply the FATF Recommendations, by examining the reports and reviews prepared by the FATF, International Monetary Fund, and the World Bank publications.

DNFBPs should note that regardless of the exemption mentioned above, DNFBPs should with respect to public companies verify that any person purporting to act on behalf of the customer is so authorized, and verify the identity of that person.

6.6 Reliance on a Third Party

Section 3F.1 of the AML Regulations 2002 provides that DNFBPs can rely on third parties to carry out CDD measures on customers and beneficial owners under Section 3B and Section 3C, if authorised by the Banking Commissioner.

Section 3F.3 of the AML Regulations provides that DNFBPs may rely on non-resident third parties to apply the measures under Section 3B and Section 3C of the AML Regulations 2002 only if the DNFBP is satisfied that:

- the third party is adequately regulated and supervised;
- the third party has measures in place to comply with the CDD and record-keeping requirements of the AML Regulations 2002;
- the third party is subject to money laundering and terrorist financial policies comparable with the FATF Recommendations;
- the thirds party is subject to licensing and supervision to enforce AML/CFT policies and it has not been subject to any material disciplinary action that call into question the execution of those policies;
- the third party is located in a jurisdiction that is effectively implementing FATF Recommendations;
- the third party is not located in the jurisdiction identified by the Banking Commissioner as a higher risk country;
- the third party is not the one that has been identified by the Banking Commissioner as non-complying with the FATF Recommendations or for whom the DNFBP has independent credible reason to believe as not complying with the FATF Recommendations; and
- the third party will be able to make available the copies of identification data and other relevant documentation relating to CDD requirements without delay, if requested

Section 3F. 6 of the AML Regulations 2002 further provides that DNFBPs that rely on third party to apply measures under Section 3B and Section 3C of the AML Regulations 2002 remain liable for any failure to apply such measures.

DNFBPs that rely on third parties to undertake CDD measures on their behalf must implement adequate measures, commensurate with the nature and size of their business, to ensure the third party's adherence to the requirements of the AML Regulations 2002. Some examples of such measures include but are not limited to:

- DNFBP should set out clear internal policies and procedures concerning the identification, assessment, selection, and monitoring of third-party relationships. These include, for instance:
    - policies and procedures for determining the adequacy of a third-party's CDD and record-keeping measures, including the evaluation of such factors as the comprehensiveness and quality of its AML/CFT policies, procedures, and controls; the number of personnel dedicated to CDD; and its audit and/or quality assurance policies regarding CDD. In this regard, DNFBPs are advised that tools such as questionnaires, scorecards, and on-site visits may be useful in evaluating the adequacy of a third party's adherence.
    - Policies and procedures on the frequency of testing performed on such third parties.
- Service-level agreements should set out the roles and responsibilities of the DNFBP and the third party and specify the nature of the CDD and record-keeping requirements to be fulfilled. The agreement should have clear contractual terms in respect of the obligations of the third party to obtain and maintain the necessary records, and to provide the DNFBP with CDD documentation or information without delay upon request. DNFBPs should ensure that the agreement should not contain any conditional language, whether explicit or implied, which may result in the inability of the third Party to provide the underlying CDD documentation or information upon request. Examples of such conditional language include (but are not limited to) terms such as 'to the extent permissible by law, 'subject to regulatory request' etc.;
- Procedures for the certification by third parties of documents and other records about the CDD measures undertaken.
- DNFBPs should only rely on the third party to carry out CDD measures required by Section 3B and Section 3C of the AML Regulations 2002. DNFBPs should not rely on the third party to fulfill the -going monitoring requirements, which they are obliged to conduct as warranted by the risk of their underlying customers, as prescribed by Section 3I of the AML Regulations 2002.
- DNFBPs should not rely on a third party to perform the enhanced CDD measures or to provide senior management approval. However, the relevant third party may assist the DNFBP in gathering the necessary documentation or information to establish the source of wealth and source of funds; and
- DNFBP should have policies and procedures in place to conduct regular assurance testing on third parties to ensure documentation can be retrieved without undue delay, and that the quality of the underlying documents obtained is sufficient as required by the AML Regulations 2002.

DNFBPs must ensure and be fully satisfied that, in placing reliance on third parties, they can meet their obligations under the AML Regulations 2002. In this regard, when placing reliance on non-resident third parties, DNFBPs must ensure that they are subject to AML/CFT regulatory and supervisory framework that is at least equivalent to the framework in the RMI. This means that DNFBPs must ensure that the third party is regulated and supervised for AML/CFT purposes, and adheres to the equivalent CDD and record-keeping measures.

DNFBPs should note that placing reliance on a third party per Section 3F of the AML Regulations 2002 does not include a situation where a DNFBP has appointed another entity to apply the necessary measures as an outsourcing service provider, intermediary, or an agent of the DNFBP. Section 3F.7 of the AML Regulations 2002 provides that "*the requirements of [Section 3F] do not apply to outsourcing or agency relationships, i.e., where the agent is acting under a contractual arrangement with the [DNFP] to carry out its CDD functions*."

7. Suspicious Activity Reporting

Suspicious Activity Reports ("SARs") play a pivotal role in the fight against ML and TF. Information provided on SARs assists the Banking Commissioner and other competent authorities in their investigations, resulting in the disruption of criminal and terrorist activities, and can ultimately result in prosecution and imprisonment. SARs also provide authorities with valuable market intelligence on trends and typologies.

7.1 Meaning of a Suspicious Transaction

Section 5(2) of the AML Regulations 2002 provides that:

"a suspicious transaction is a transaction conducted or attempted by, at, or through [a DNFBP] that [a DNFBP] knows, suspects, or has reason to suspect that:

- *(a) involves funds or other assets that are the proceeds of crime or are otherwise derived from illegal activity, including, but not limited to, tax matters; or*
- *(b) was intended, conducted, or attempted to be conducted:*
  - *(i) in order to hide or disguise funds or assets that are the proceeds of crime or are otherwise derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets); or*
  - *(ii) as part of a plan to violate or evade any Marshall Islands law or regulation or to avoid any transaction reporting requirement under Marshall Islands law or regulation; or*
- *(c) involves a transaction or transactions which:*
  - *(i) is/are complex or unusual; or*
  - *(ii) present an unusual pattern; or*
  - *(iii) has/have no apparent economic or lawful purpose; or*
  - *(iv) is/are not the sort of transaction in which any person or entity involved would normally be expected to engage; or*
- (d) *could constitute or be related to terrorist financing, terrorist acts, a terrorist organization, an individual terrorist or to terrorist property or proliferation financing."*

It should be noted that for a transaction to be considered a 'suspicious transaction', a DNFBP should either 'know', 'suspect', or 'has reason to suspect that it relates to any conditions referenced under Section 5(2)(a) to 5(2)(d). The suspicious nature of a transaction can be inferred from certain circumstances and information, including suspicious indicators, behavioral patterns, or CDD information, and it is not dependent on obtaining evidence that a predicate offense has been committed or on proving the illicit source of the funds involved. DNFBPs do not need to know the underlying criminal activity nor any founded suspicion that the proceeds originate from criminal activity – reasonable grounds to suspect are sufficient.

7.2 Requirement to Report

Under the AML Regulations 2002, all DNFBPs are obliged to report suspicious transactions to the Banking Commissioner, subject to the qualifications provided under Section 10(b) of the Regulations.

Section 10(b) of the AML Regulations 2002 provides that:

"The requirements to report suspicious transactions set out in Section 5 of [the] Regulations apply to all DNFBPs, subject to the following qualifications:

(1) Dealers in precious metals or stones – the requirements of Section 5 apply when they engage in a cash transaction with a customer of $15,000 or more.

(2) Lawyers, notaries, other independent legal professionals and accountants – the requirements of Section 5 apply when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in subparagraph (b)(1)(iv) of this Section unless the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.

(3) Trust and company service providers – the requirements of Section 5 apply when, on behalf or for a client, they engage in a transaction in relation to the activities described in subparagraph (b)(1)(iv) of this Section. could constitute or be related to terrorist financing, terrorist acts, a terrorist organization, an individual terrorist or to terrorist property or proliferation financing.

To fulfill their SAR-related obligations under the AML Regulations 2002, DNFBPs should implement adequate internal policies, procedures, and controls for the identification and reporting of suspicious transactions, both internally and externally.

7.3 Identification of Suspicious Transactions

When assessing potential suspicious transactions, DNFBPs should note that to be considered a suspicious transaction, a transaction need not be completed, in progress, or pending completion transaction. Attempted transactions, a transaction that is not executed, and past transactions (regardless of their timing or completion status), which are found to raise reasonable grounds for suspicion, must be reported following the relevant requirements.

In addition, DNFBPs should note that there is no minimum monetary threshold for reporting and no amount should be considered too low for suspicion. This is particularly important when considering potential terrorist financing transactions, which may often involve very small amounts of money.

Commensurate with the nature and size of their business, DNFBPs should determine the internal policies, procedures, and controls that they apply to identify and evaluate potential suspicious transactions, including putting in place indicators that can be used to identify any suspicious transactions. DNFBPs should refer to Schedule 1 of the AML Regulations 2002 which provides a list of higher-risk situations relating to customers, country or geographical areas, particular products, services, transactions, and delivery channels. Nonetheless, DNFBPs should consider their specific products, services, and customers when deciding on suspicion, as what might be considered suspicious for one product, service or customer may not be for another. They must also refer to the RMI's national risk assessment, any sectoral or thematic risk assessment, and their business-level ML/TF risk assessment in this regard.

The suspicious indicators should be updated on an ongoing basis following any instructions by the Banking Commissioner, as well as in keeping with the relevant developments concerning ML/TF typologies and trends.

The following is a non-exhaustive list of examples of what might raise suspicion:

- Transactions or a series of transactions that appear to be unnecessarily complex, making it difficult to identify the beneficial owner;
- Transactions that do not appear to make economic sense or have an apparent lawful purpose;
- Transaction activities (in terms of both amount and volume) that do not appear to be in line with the expected level of activity for the customer and/or are inconsistent with the customer's previous activity;
- Transactions above a customer's stated income or your knowledge of the customer's occupation, business, or activity;
- Large unexplained cash transactions;
- Requests for third-party payments that do not make sense or have any rationale;
- Transactions involving high-risk jurisdictions, particularly in circumstances where there is no obvious basis or rationale for doing so;
- Frequent or unexplained changes in ownership or management of business relationships;
- Refusal to provide customer due diligence documentation or provide what appears to be forged documentation.

7.4 Timing to file a SAR

Section 5(b)(3) of the AML Regulations 2002 requires DNFBPs to file a SAR … "*no later than three (3) working days after the date of initial detection by the [DNFBP] of facts that may constitute a basis for filing a SAR*." It further provides that "*if no suspect was identified on the date of the detection of the incident requiring the filing, a [DNFBP] may file a SAR and submit an additional SAR (referencing the first) when such information becomes available."*

Section 5(b)(4) of the AML Regulations 2002 states that:

"[*i*]*n situations involving violations that require immediate attention, such as, for example, ongoing money laundering, terrorist financing … the [DNFBP] shall immediately notify the Banking Commissioner, or his designee, in addition to a later filing of the SAR within the 3 working day timeframe*."

DNFBPs should note that in the case of non-identification of a suspect on the date of detecting suspicious activity, they should at least file a SAR with the Banking Commissioner within 3 days of such initial detection and later submit any additional information, as it becomes available.

7.5 Internal SARs

DNFBPs should establish adequate internal policies, procedures, and controls for the identification and internal reporting and escalation of suspicious transactions. In this regard, DNFBPs should ensure that:

- Operational procedures for staff on filing an internal report ('internal reporting procedures') are adequately documented. For example, the internal reporting procedures should include at least:
    - All required steps for the reporting of suspicions from staff to the Compliance Officer and from the Compliance Officer to the Banking Commissioner;
    - The conditions, timing, and methods to file internal SARs;
    - Content requirement and format to file internal SARs;
    - Formal acknowledgment by the DNFBP's Compliance Officer or any other person(s) charged under the DNFBP's internal reporting process with investigating suspicions raised internally by staff;
    - Procedures related to the provision of additional information, follow-up actions relating to the transactions, and handling of business relationships after filing an internal SAR;
    - Information concerning ' Tipping-off' to ensure that staff are aware of their obligations under the AML Regulations, the penalties for the offense of Tipping Off and that they exercise caution after the filing of an STR;
    - Policies and procedures for the analysis and decision-making of suspicious transactions by the Compliance Officer in regards to reporting to the Banking Commissioner.
- AML/CFT training provided to staff includes details on the DNFBP's internal reporting procedure as well as details on the reporting of suspicions to the Banking Commissioner;
- There are no discrepancies between internal reporting procedures as documented and operational practices. For example, where the DNFBP's internal reporting procedure states that suspicions are to be escalated using an internal reporting form then the raising of suspicions should not be conducted verbally;
- Where a DNFBP utilizes a transaction monitoring system, there is a regular review of the correlation between alerts generated from the system and the reporting of suspicious transactions to the Banking Commissioner. DNFBPs should ensure that they have an adequate process and dedicated, experienced staff for the investigation of and dealing with system-generated alerts. The investigation of alerts and the conclusion of the investigation should be documented, including the decision to close the alert or to promptly report the transaction as suspicious;
- Where a suspicion has been escalated for further assessment and review, the DNFBP's records provide sufficient detail of the assessment and adjudication, giving rise to the decision to file or not file a report to the Banking Commissioner. For example:
    - the circumstances that gave rise to the suspicion;
    - the assessment or additional analysis that took place; and
    - the rationale for the decision not to file or the basis for making a report to the Banking Commissioner.
- Sufficient information is retained to record the reported suspicion, and support the DNFBP's determination of whether to discount the suspicion or to proceed and file the SAR with the Banking Commissioner.

7.6 Procedures to file SARs with the Banking Commissioner

Section 5(b)(2) of the AML Regulations 2002 provides that reports in relation to money laundering and terrorist financing suspicions shall be filed with the Banking Commissioner by completing a SAR form, pursuant to the instructions given in the form.

To comply with their suspicious activity reporting requirements to the Banking Commissioner, DNFBPs should establish adequate internal policies, procedures, and controls for the identification and internal reporting of suspicious transactions including the provision of the necessary records and data, to the designated Compliance Officer for further analysis and reporting decisions, as well as for reporting the suspicious transaction by the Compliance Officer to the Banking Commissioner (as discussed above in section 7.5).

DNFBPs should ensure that SARs submitted to the Banking Commissioner are sufficiently detailed to assist the authorities in their analysis and investigations and strictly follow the instructions as provided in the SAR form

Where a SAR has been returned to a DNFBP by the Banking Commissioner (due to either incomplete information or for any other reason), a DNFBP should take the necessary action required to update the SAR, and resubmit the SAR to the Banking Commissioner, as soon as practicable.

7.7 Confidentiality and Prohibition against "Tipping Off"

Section 5(d) of the AML Regulations 2002 provides that "*[DNFBPs], its employees, officers, directors, and agents shall not notify any person or entity other than those authorised by law that a suspicion has been formed or that a SAR or related information is being or has been filed in accordance with this Section 5.*"

DNFBPs and their staff, including agents, are obliged to maintain confidentiality concerning both the forming of suspicion or the act of reporting a suspicious transaction or related information internally or externally.

As per their risk-based AML/CFT program, and in keeping with the nature and size of their business, DNFBPs should establish adequate policies, procedures, and controls to ensure the confidentiality and protection of data and information related to SARs. DNFBPs must ensure that all relevant information relating to STRs is kept confidential, with due regard to the conditions provided for in the law, and the guiding principles for this must be established in policies and procedures. DNFBPs need to ensure that their policy and procedures should reflect, for example, appropriate access rights concerning core systems used for case management and notifications, secure information flows, and guidance/training to all staff members involved. his guidance and training are primarily important for the first-line staff who have contact with customers. These staff must know when there may be cases of suspicious transactions, what questions they have to ask the customer, and which information they must not under any circumstances disclose to the customer.

DNFBPs should include details on the offense of 'Tipping-off', the need for staff to exercise caution, and the penalties for the offense within the DNFBP's internal AML/CFT policies and procedures. DNFBPs should include as part of their AML/CFT training to all staff, advice around the treatment of unusual transactions and additional due diligence measures, which should be taken by staff without committing the offense of 'Tipping -off.

8. Record Keeping

8.1 Obligations for Retention of Records

Adequate record keeping is vital to the preservation of the audit trail, which in turn can assist with any investigations of money laundering and terrorist financing.

DNFBPs are obliged to maintain detailed records, documents, data, and statistics for all transactions, all documentation and information obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, as well as a variety of record types and documents associated with their business-level ML/TF risk assessment and mitigation measures, as specified in the relevant provisions of the AML Regulations 2002. DNFBPs are required to maintain the records in a readily recoverable manner to be accessible within a reasonable period and made available to the Banking Commissioner or other competent authorities on a timely basis and in no event later than five(5) working days.

The statutory retention period for all records (except in the case of SARs) is a minimum of six (6) years from the date of the most recent of any of the following events:

- termination of the account or business relationship;
- completion of the transaction or occasional transaction (in respect of customers with whom no business relationship is established);

For SARs, DNFBPs are required to maintain records for fifteen (15) years from the date of filing the SAR to the Banking Commissioner.

DNFBPs should note that, if considered appropriate, the Banking Commissioner may require the retention of records of any DNFBP for a longer period than stated in the AML Regulations 2002.

DNFBPs should ensure that their internal AML/CFT policies and procedures contain sufficient details of their record-keeping obligations under the AML Regulations 2002. The adequacy and detail of records to be kept by a DNFBP should be reflective of the nature, scale, and complexity of the business of a DNFBP. DNFBPs should also ensure that all their employees including agents and outsourced service providers are aware of, and adhere to, the DNFBP's procedures on record keeping.

Effective record-keeping allows DNFBPs to demonstrate to the Banking Commissioner the steps they have taken to comply with their obligations under the AML Regulations 2002.

8.2 Required Record Types

DNFBPs are required to retain records in relation to the following:

- Business-level ML/TF risk assessments (under Section 10(3) of the AML Regulations 2002);
- Customer and customer's beneficial owners' information (under section 3B.8 and 3C.8 of the AML Regulations 2002);
- Transactions (under section 4 of the AML Regulations 2002)
- Suspicious Activity Reports (under section 5(c) of the AML Regulations 2002);

DNFBPs should also retain records *inter alia* concerning the following:

- Reliance on third parties to undertake CDD;
- Ongoing monitoring of business relationships;
- Minutes of Board meetings;
- Evidence of all matters requiring senior management approval under the AML Regulations 2002; and
- Training of their relevant employees.

8.2.1 Business-level ML/TF Risk Assessment

DNFBPs must document and record their business-level ML/TF risk assessments in writing, including any changes made to the risk assessment as part of their review and monitoring process. Such an approach ensures that DNFBPs can demonstrate that their business-level ML/TF risk assessment and associated risk management measures are up-to-date and adequate.

8.2.2 Customer Information

DNFBPs must maintain adequate records of all their customers, whether individuals, legal persons, or legal arrangements, including:

- All documentation and information obtained to identify and verify a customer, the person(s) authorized to act on behalf of the customer, and any beneficial owners;
- All customer risk assessments and profiling records;
- Copies of all additional documentation and information obtained, where EDD measures have been applied to a customer or customer's beneficial owner. A DNFBP should also ensure that they document their rationale for applying EDD measures;
- Evidence of any sample testing of CDD files, which the DNFBP has undertaken as part of its assurance testing process; and
- Copies of documentation and information were obtained as part of the DNFBP's ongoing monitoring process.

8.2.3 Transactions

DNFBPs should be cognisant of the importance of the obligations under Section 4 of the AML Regulations 2002 to retain copies of all transactions carried out for or on behalf of a customer by the DNFBPs for their internal audit purposes as well as any possible investigations by law enforcement.

DNFBPs must retain the operational and statistical records, documents, and information concerning all transactions executed or processed by the DNFBP, whether domestic or international and irrespective of the type of customer and whether or not a business relationship is maintained, for a minimum period of six (6) years. Some examples of documents and information which should be obtained and retained by DNFBPs relating to transactions include, but are not limited to:

- Customer correspondence, requests, or order forms related to the initiation and performance of all types of transactions and related agreements;
- Customer payment advice, receipts, invoices, billing notifications, statement of accounts, expense reimbursement requests or notifications;
- Sale, purchase, merger-acquisition, and similar agreements;
- Statistical and analytical data related to customers' financial transactions, including their monetary value, volumes, currencies, interest rates, and other information.

DNFBPs must also maintain a record of all occasional transactions exceeding $10,000 or its equivalent in a foreign currency.

In addition to the above, DNFBPs must compile and maintain notes and their findings on any particularly complex, large, or unusual transactions, and keep these findings as a part of their records.

8.2.4 Suspicious Activity Reports (SARs)

DNFBPs must keep sufficient records concerning SARs, including :

- the circumstances that gave rise to the suspicion;
- any additional monitoring/assessment that was undertaken;
- the findings of the assessment or investigations performed;
- whether the suspicion was reported/not reported, and
- rationale for reporting or not reporting to the Banking Commission.

DNFBPs must retain copies of all documentation and information used as a part of any internal assessment of a customer or business relationship, following on from the filing of an internal SAR by a staff member of the DNFBP.

DNFBPs must retain records to provide evidence and justification behind their decision on whether or not to file a SAR with the Banking Commission. In this regard, DNFBPs must also retain copies of the supporting documentation and information, that assisted them in reaching their decision.

Where a DNFBP has filed a SAR to the Banking Commission, it must retain a copy of the original SAR filed to the Banking Commission, as well as any supporting documentation to reach its decision for fifteen (15) years from the date of filing the SAR with the Banking Commissioner.

8.2.5 Reliance on Thirds Parties to Undertake CDD

DNFBPs should ensure when placing reliance on third parties to undertake CDD, that there is a written arrangement in place between the DNFBP and the third-party provider with clear contractual terms in respect of the obligations of the third party to obtain and maintain the necessary records, and to provide the DNFBP with CDD documentation or information without delay when requested.

The DNFBPs must ensure that the third parties adhere to the record-keeping requirements of the AML Regulations 2002. To fulfill their obligations under the AML Regulations 2002, and commensurate with the nature and size of their businesses, DNFBPs should determine the appropriate policies, procedures, and controls related to the assessment, monitoring, and testing of third parties record retention frameworks. Such policies, procedures, and controls should be documented and communicated to the appropriate levels of the organization. Some of the factors that DNFBPs should consider when formulation relevant policies, procedures, and controls include, but are not limited to:

- Organizational roles and responsibilities concerning the assessment, monitoring, and testing of the third party's policies, procedures, and controls related to record-keeping and data protection, including appropriate business contingency and escalation procedures;
- Organizational roles and responsibilities for the implementation of service-level agreements with third parties governing the provision of record-keeping services;
- Operational procedures related to request and transfer of records and documents, as well as their physical and cyber security, and the protection of active and archived data and records from unauthorized access;
- Appropriate audit and quality assurance testing policies related to the monitoring and testing of the third-party's record-retention framework

8.2.6 Ongoing Monitoring of Business Relationships

DNFBPs must retain all records to verify and provide evidence of the ongoing monitoring conducted by the DNFBP, including the monitoring of transactions, the results of such monitoring, and decisions taken as a result of ongoing monitoring.

8.2.7 Minutes of Board meetings

DNFBPs should retain records of all meetings and decisions made at the Board level concerning:

- how the requirements of the AML Regulations 2002 were assessed and implemented; and
- any AML/CFT issues as they arise on an ongoing basis.

8.2.8 Evidence of all matters requiring senior management approval

DNFBPs should ensure that appropriate evidence is retained following its record retention policy regarding the DNFBP's obligations concerning all matters requiring senior management approval under the AML Regulations 2002.

8.2.9 Training

DNFBPs should retain records of all AML/CFT training provided to staff during a given year. Information should include:

- the dates on which AML/CFT training was provided to staff;
- attendance and sign-in sheets (where relevant) of who received the AML/CFT training;
- the nature and content of the AML/CFT training provided; and
- results of the assessment and examination during the training session.

8.3 Timeframe for the Availability of Records

DNFBPs are required to maintain all the records in a readily recoverable manner to be accessible within a reasonable period, and to make them available to the Banking Commissioner or other competent authorities on a timely basis, in no event later than five(5) working days.

Where the identification and verification records are held outside of the Marshall Islands, it is the responsibility of the DNFBP to ensure that the records available meet the requirements under the AML Regulations 2002, including their availability without delay, when requested.

Section 3F.3 of the AML Regulations provides that when DNFBPs relies on non-resident third parties for conducting CDD measures, they shall be satisfied that third parties have adequate measures in place to comply with the CDD and recordkeeping requirements in the AML Regulations 2002.

Section 3F.4 of the AML Regulations 2002 provides that the if DNFBPs relies on third parties for conducting CDD measures, they must take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available without delay, if requested.

DNFBPs should ensure that no secrecy or data protection legislation should restrict access to the records by the DNFBP on request, which should be made available without delay. If it is found that such restrictions exist, copies of the underlying records of identity and other documentation should be sought and retained within the Marshall Islands. In such instances, the contractual arrangements between the DNFBP and the third party should provide for immediate availability of copies of identification data and other relevant CDD documentation from third parties.

DNFBPs should take account of the scope of AML/CFT legislation in other countries and should ensure that records kept in other countries that are needed by the DNFBP to comply with AML Regulations 2002 are retained for the required period.

9. Annexes

9.1 Glossary of Terms

The following terms are used throughout the Guidelines:

AML	Anti-Money Laundering
AML/CFT	Anti-Money Laundering and Countering the Financing of terrorism
APG	Asia Pacific Group on Money Laundering
CDD	Customer Due Diligence
DNFBPs	Designated Non-Financial Businesses and Professions
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FSRBs	FATF-Style Regional Bodies
FIU	Financial Intelligence Unit
ML	Money Laundering
ML/TF	Money Laundering/Terrorist Financing
NRA	National Risk Assessment
PEPs	Politically Exposed Persons
PF	Proliferation Financing
RBA	Risk-based Approach
RMI	Republic of Marshall Islands
SARs	Suspicious Activity Reporting
SDD	Simplified Due Diligence
TCMI	Trust Company of the Marshall Islands
TF	Terrorist Financing
TFS	Terrorist Financial Sanctions
VA	Virtual Asset
VASP	Virtual Asset Service Provider

Any term used in the Guidelines should be construed in accordance with its definition under the Banking Act 1987 and AML Regulations 2002.

9.2 Useful Links

APG	http://www.apgml.org
Egmont Group	https://egmontgroup.org
FATF	http://www.fatf-gafi.org
Interpol/ML	https://www.interpol.int/Crimes/Financial-crime
Office of the Banking Commission, RMI	http://www.rmibankingcomm.org/
UNODC	https://www.unodc.org/unodc/en/money-laundering/index.html?ref=menuside