The Republic of Nauru

2022 - 2025

National Strategy for Anti-Money Laundering and Combatting the Financing of Terrorism

This 2023 print is a revision of the Strategy issued on 1st July 2022

Table of Contents

Acronyms

AML Act	Anti-Money Laundering Act 2008
AML/CFT	Anti-Money Laundering and combatting the Financing of Terrorism
AMLGC	Anti-Money Laundering Governance Council
AMLOC	Anti-Money Laundering Officials Committee
AMLPPC	Anti-Money Laundering Private Partner Committee
APG	Asia Pacific Group on Money Laundering
FATF	Financial Actions Task Force
FIU	Financial Intelligence Unit
ME	Mutual Evaluation
NCC	Nauru Chamber of Commerce
NRA	National Risk Assessment
PPP	Public Private Partnership
RON	Republic of Nauru
STR	Suspicious Transaction Report
UNSCR	United Nations Security Council

Foreword

On behalf of the Government of Nauru, I am pleased to present *'The Republic of Nauru National Strategy for Anti-Money Laundering and Combatting the Financial Terrorism* 2022-2025' (Strategy). The aim for this Strategy is to provide general education, guidance, implementation and enforcement of the Republic of Nauru's international commitment as a global member in combatting and condemning money laundering, terrorist financing, proliferation financing and other financial crimes. The illicit manoeuvring and movement of funds obtained through illegitimate means and then circulated in our national and international financial system poses serious socio-economic and global security risks. The magnitude of the original crimes is severe in itself, but they also trigger other crimes, which includes the undermining of the rule of law, governance with transparency and integrity and economic and financial instability.

The principal crimes have resulted in members of United Nations implementing various multilateral instruments. To name a few are the *Vienna Convention (1988) against Illicit Traffic in Narcotic Drugs and Psychotropic Substances; the Palermo Convention (2000) against Transnational Organized Crime; Convention for the Suppression of Financing of Terrorism (1999).* These have been further complimented by various UNSCRs to criminalize money laundering, terrorist financing, proliferation financing and other financial crimes. The Republic is a member of the Conventions and is also bound by the UNSCRs.

In addition to these instruments, there are FATF recommendations. Currently there are 40 recommendations. The Republic finds FATF recommendations extremely important in establishing its national standards to address money laundering, terrorist financing, proliferation financing and other financial crimes. Nauru joined as a member of the APG in 2007 following enactment of its first *Anti-Money Laundering Act 2004.* In 2012, mutual evaluation was undertaken for Nauru's capability on addressing money laundering, terrorist financing and proliferation financing and other financial crimes.

In taking its obligations seriously, despite not having formal financial institutions for more than a decade since 2004, Nauru maintained the office of FIU. In the past 10 years, the office has been further strengthened. Considering Nauru being a small country, maintaining independence of the FIU is very critical. For that reason, the Government approved that the head of the FIU be an expatriate. The Strategy must not only incorporate but undertake capacity building for the future to allow local Nauruan's to transition expatriate staff once an integrated and inter-sectoral implementation of the Strategy is substantially embedded.

The United Nations Resolutions, International and Regional agreements in combating money laundering, terrorist financing, proliferation financing and other financial crimes have been domesticated in the national laws. The *Anti-money Laundering Act 2004* was repealed and replaced by the current 2008 Act. Over time it has been amended a few times as well. Currently, consultations are under way to review to amend or repeal and replace the 2008 Act incorporating the current and most updated requirements for the deterrence of money laundering, terrorist financing, proliferation financing and other financial crimes. Various other laws supporting the enforcement of the AML/CFT has been enacted by four different Governments of Nauru since the last mutual evaluation. This demonstrates a collective national commitment at the highest political level, irrespective of differences in political ideologies and other matters. The political will of the

Government has seen the opening of a financial institution in Nauru in 2015, the Bendigo Banking Agency. The introduction and enforcement of taxation regime through legislation for personal income and business profits since 2014, undoubtedly paves way for greater accountability of the movement of money in and outside of the economy. Stricter border control on the means, mode and quantum of currency movement through legislation and cabinet decisions prohibit illegal conveyance of money to and from the Republic. Electronic transaction and online shopping are becoming matters of immediate concern, which the National Strategy 2022- 2025 must address, as it is progressively implemented. The current issue of retaining cash in the economy is a concern for the Government. It needs cash to be available in Nauru for use by people for purchasing of goods and services. The Strategy must compliment the Government's goal to ensure that there is no illicit removal of currency from Nauru by travellers, businesses and visitors. Even where currency is to be moved lawfully, appropriate border control measures must be put in place and enforced. The Strategy must contain measures to educate the public on this.

Cash control mechanisms are to be put in place by the Government. The Bendigo Bank Agency plays a significant role now. The introduction of Automatic Teller Machines and Electronic Fund Transfer have all contributed to records being generated and collated of money. Also, it is to restrict movement of physical cash from Nauru.

This Strategy is intended to take a holistic government approach for the preparation for the ME in 2023. A greater collaboration and co-operation is established through the AMLGC and AMLOC. In ensuring that legislative and administrative mechanisms are enforced, the FIU has been given administrative support to act independently. The Strategy must develop plans for financial independence of FIU, through grant funding or national budget. Focus must also be given to enable FIU independence in carrying out its functions and powers in legislation in the future.

A particular focus of the Strategy during this period is to undertake all preparatory work for Nauru to join the ***Egmont Group.*** Joining a broader community, which has a common goal of combatting money laundering, terrorist financing and proliferation financing and other financial crimes, will no doubt enhance our role in the global financial community.

An area, which has become necessary for Nauru to consider is the targeted financial sanctions. This is a UN Resolution requirement no 1267 and successor UNSC resolutions. The Strategy must see to the domestication of this in our laws and administrative procedures of all stakeholders.

With this in mind, I approve this Strategy and it is to come into effect from 1st July 2022.

Jay Udit

Chairperson of the Anti-Money Laundering Governance Council

Introduction

1. The Republic of Nauru is a member of the APG. The APG is a non-political intergovernmental organization established in 1997. Its existence is through the member countries commitments. The Republic joined the APG in 2007. Since becoming a member, the Republic has continued to improve on its technical compliance and effectiveness of obligations for complying with FATF recommendations, money laundering, terrorism financing, proliferation financing and other financial crimes.

2. There are currently 40 FATF recommendations. The Secretariat of APG works with the member countries for the implementation of the recommendations. As a member, the Republic is committed to combatting money laundering, terrorism financing, proliferation financing and other financial crimes through our continuous efforts to monitor and identify emerging threats and vulnerabilities. The Republic will continue to develop and implement a risk-based approach to risks. The 40 FATF recommendations are annexed to this Strategy.

3. The Republic has undertaken this by ensuring that the FATF recommendations are incorporated in domestic legislation or other administrative measures. In addition, due to the nature of offences, the Republic has laws which does not only have domestic but extraterritorial effect.

4. An effective system shall create and maintain the integrity and reputation of the Republic's Financial system. Such a system is a crucial component of fulfilling the Republic's vision under the National Sustainable Strategy (2019-2030). In particular:

A. National Vision: A future where individual, community, business and government partnerships contribute to a sustainable quality of life for all Nauruans.
B. Goal: Stable, economically and fiscally responsible government.
C. Goal: Development of an economy based on multiple sources of legitimate revenue.

Purpose

5. The purpose of this document is to formalise the Republic's Strategy for anti-money laundering, and combatting the terrorism financing, proliferation financing and other financial crimes and to clearly set out the goals and objectives of the Strategy.

6. Together with the domestic laws, this Strategy is the policy statement of our framework for anti-money laundering and combatting the terrorism financing, proliferation financing and other financial crimes. Furthermore, this Strategy coincidentally falls within the period for the Republic's second ME. It gave the Republic the opportunity to review its current legislation and administrative framework to not only meet its international obligations but to bring better cooperation amongst different agencies and stakeholders.

Methodical Approach to Implementation

7. The Strategy is developed to address threats and vulnerabilities identified in the 2012 ME report, 2018 NRA and the legislative gap analysis 2018. Since the 2012 ME, the Republic has undergone major reforms in its framework including amendments to and enactment of new laws to meet the FATF requirements. Other legislative changes have also been introduced which directly or indirectly support the work of the FIU.

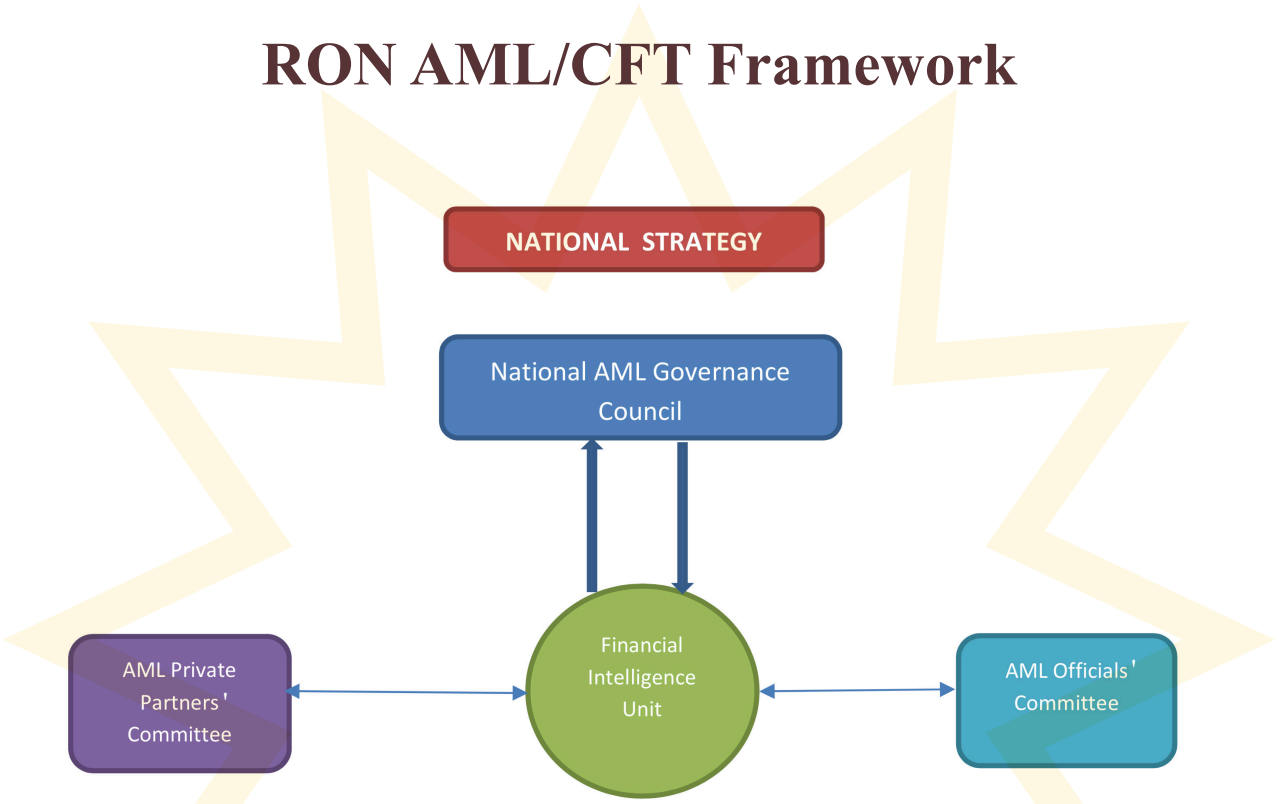
8. Both the 2012 ME and 2018 NRA identified high and low risk areas and this Strategy is designed to address risks through a collaborative and risk-based approach.

9. The Strategy promotes stakeholders both in public and private sectors to work in partnership to implement the Strategy. This approach is consistent with the PPP that is promoted by the APG and similar bodies[1] aligned to the FATF.

[1]Caribbean Financial Action Task Force - regional body for the Caribbean groups and Eastern and Southern African Anti - Money Laundering Group.

Republic's Strategy Framework

10. The chart below represents the RON's AML/CFT organisational framework.



National AML Governance Council (AMLGC)

11. The Strategy establishes the National Anti-Money Laundering Governance Council ('Council'). Included in the Council are the Secretary for Justice, Secretary for Finance, Commissioner of Police and Director of Public Prosecutions. The FIU together with its Supervisor provide secretariat support to the Council. The role of the Council is to provide an oversight in the collaboration amongst the different stakeholders.

AML Officials Committee (AMLOC)

12. The AMLOC comprise of key public sector stakeholders who are in the forefront of monitoring of the risks and exposure of the Republic to money laundering, terrorist financing, proliferation financing and other financial crimes. These includes representatives from the Nauru FIU, Nauru Police Force, Nauru Customs Service Office, Nauru Revenue Office, Department of Justice and Border Control, Department of Environment, Nauru Fisheries and Marine Resources Authority and Department of

Foreign Affairs. The role of the Committee is to meet regularly to discuss and share strategies on risks identified, information and contribute ideas at a national level. It is responsible for implementing their obligations within their respective departments or organisations. They shall conduct awareness internally and contribute to improving the Republic's AML/CFT framework.

AML Private Partners' Committee

13. Information sharing is a critical factor in ensuring an effective implementation of the AML/CFT framework for the Republic. The involvement of the private sector to work in collaboration with the public sector can contribute to a better understanding of AML/CFT risks. The private sector is most vulnerable and at the forefront of being targeted for AML/CFT contravening activities. They are equally responsible for and have a legal obligation to identify and address the risks.

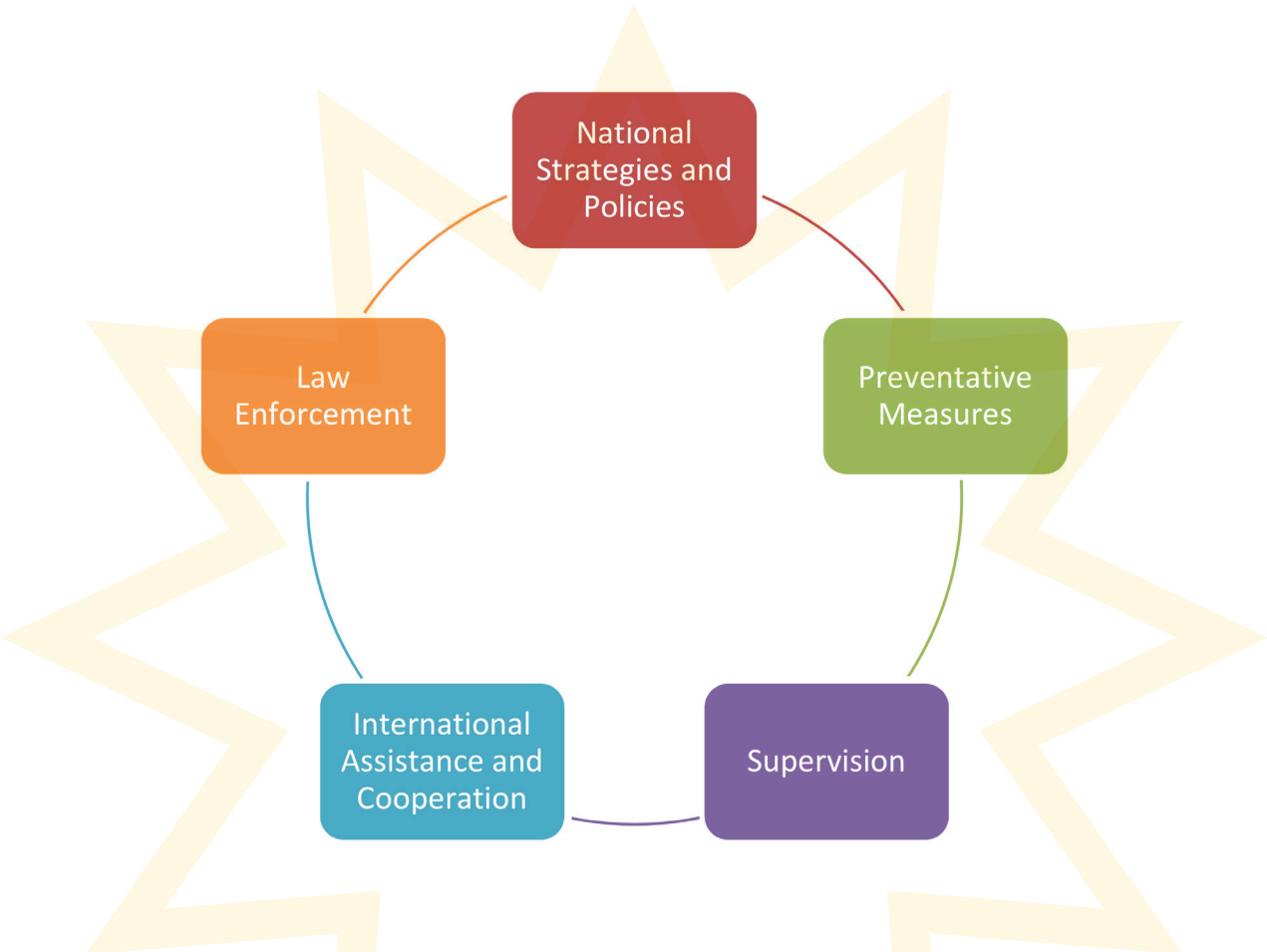
14. Thus, a collaborated approach can also allow supervisors, law enforcement agencies and private partners to share their findings and apply a risk-based approach.

15. The NCC was recently registered as an association under the *Registration of Associations Act 2020.* The NCC is an association which is formed by persons who are carrying out commercial activities in Nauru. As a collective association, it has become easier to collect and disseminate information and also to collate collective views and opinions.

16. The AMLOC and the AMLPPC members shall form the PPP.

The Republic's Strategy 2022-2025

17. The Republic has adopted a five-pillar Strategy required under the FATF Standards. The five pillars are depicted in the chart below:



18. In adopting this five-pillar strategy, the Republic has taken into account the core principles which are:

- risks within the Republic are identified, managed and mitigated;
- the Republic has to work with limited resources and capacity;
- a collaborative and common-sense approach is required from law enforcement agencies, regulators/supervisors as well as the private sector to address AML/ CFT risks; and
- that whilst the various government agencies and private sector agencies are faced with competing priorities, where possible, appropriate issues should be considered.

19. The 2018 NRA together with a powerful risk identification and assessment of AML/ CFT risks for the Republic forms the key component of this Strategy.

The Republic of Nauru | 10

Objectives

20. The Republic will focus on the following key objectives during the period 2022-2025 to mitigate AML/ CFT risks through this Strategy:

- ***Objective 1*** – Improve the AML/CFT framework to detect, disrupt and prevent AML/ CFT contravening activities.
- ***Objective 2*** – Develop and improve the effectiveness of AML/ CFT investigation and prosecution and asset forfeiture mechanisms.
- ***Objective 3*** – Strengthen domestic and international co-operation for AML/ CFT.
- ***Objective 4*** – Strengthen awareness raising and capacity building of AML/ CFT contravening activities.
- ***Objective 5*** – Develop, promote and improve data collection on AML/ CFT issues by sectors.

Objective 1

21. Improve the framework to detect, disrupt and prevent AML/ CFT contravening activities.

Goal	Action
Review and introduce new legislation to improve the technical compliance and effectiveness in detecting, disrupting and preventing AML/ CFT contravening activities. This includes a new AML Act. The proposed Act will include targeted financial sanctions.	• Legislative review project is ongoing under technical assistance from APG. • Assist sectors (both public & private) to introduce internal policies. • Encourage collaborative approach by public and private sectors. • Review Border Currency Reporting Framework.
Establish the AML Officials Committee and sub working groups for coordinating and reporting AML/CFT contravening activities.	• Develop Terms of Reference for the AMLOC. • Develop Terms of Reference for the AMLPPC. • Encourage coordination of activities between AMLOC and the AMLPPC. • Encourage active participation and information sharing in committee meetings. • Promote, encourage and create awareness on STRs. • Promote a culture of compliance.

Develop Risk Assessment mechanism.	• Introduce a NRA plan. • Introduce a NRA policy. • Contribute to regional and international forums on threats. • Monitoring ongoing developments and trends on AML/CFT risks. • Developing means to deal with the trending AML/CFT risks.
Enhance supervision framework.	• Introduce onsite and offsite supervision of reporting entities by the FIU for AML/CFT. • Implement thematic review triggers for supervision based on data analysis. • Introduce risk-based supervision.

Objective 2

22. Develop and improve the effectiveness of AML/CFT investigation and prosecution and asset forfeiture mechanisms.

Although currently there is no such case of asset forfeiture, the Republic intends to keep this updated to meet any request from other AML/CFT jurisdictions.

Goal	Action
Promote investigation, prosecution and asset forfeiture.	• Train Law Enforcement Agencies to identify cases for AML/CFT investigations. • Enhance the quality of operational analysis by FIU. • Develop Border Currency Reporting Standard Operating Procedures. • Encourage parallel financial investigations. • Identify opportunities to increase technical expertise and skills for financial investigations and asset recovery for investigators and prosecutors. • Identify suitable training through technical assistance, workshops and conferences.
Implement CFT capabilities.	• Establish a committee for Terrorism related activities including CFT and Targeted Financial Sanctions (TFS). • Identify and address TFS with technical assistance from experts. • Continue the development of trained/specialized investigators and prosecutors through training to enable investigation and prosecution of terrorist financing or proliferation financing if such a case was to arise.

Objective 3

23. Strengthen international and domestic co-operation for AML/CFT.

Goal	Action
Promote domestic cooperation amongst competent authorities.	• Ensure that the AML Officials Committee meet regularly with set AML/CFT goals for information sharing. • Promote responsibility and accountability of domestic competent authorities for AML/CFT actions. • Formalise the establishment of ad-hoc working group at operational levels to address needs as they arise. • Encourage where possible for the use of technology to enhance cooperation such as use of shared databases where appropriate.
Promote international cooperation amongst competent authorities.	• Entering into bilateral or multilateral arrangements with other countries, financial intelligence units or similar body. • Establish relationship for information sharing with foreign agencies. • Establishing systems to maintain confidentiality of information provided by other jurisdictions. • Join EGMONT Group.

Objective 4

24. Strengthen awareness raising and capacity Building of AML/CFT contravening activities.

Goal	Action
Raise awareness on AML/CFT for all stakeholders (public and private sector) including the public.	• Use the AMLOC and the AMLPPC as a base for creating awareness in public and private sectors on AML/CFT. • Conduct regular awareness to all sectors with a program. • FIU to educate the public and create awareness on AML/CFT activities. • Issue alert notices and guidelines on key AML/CFT activities as and when required. • Promote an understanding and regular sharing of information as a means to disseminate information on AML/CFT issues • Utilising the cooperation and understanding of all stakeholders to make awareness of any STRs.

Use of technology for AML/CFT awareness.	• Develop FIU Website for easy access of AML/CFT information for stakeholders, public and online reporting. • Use media such as Nauru Media, Radio and internet for distribution of awareness material for AML/CFT. • Use of social media such as the official Government of Nauru Facebook page for AML/CFT awareness.
Utilise opportunities to develop skills and capacity of law enforcement agencies.	• Promote inter agency training on AML/CFT issues with a focus on shared experiences, on the job learning in addressing the Republic's AML/CFT risks. • Encourage online self-paced training on AML/CFT which is offered without cost by international organizations. • Identify training on technical skills (analytical and supervisory) with technical assistance from regional and international partners and donors.

Objective 5

25. Develop, promote and improve data collection mechanism on AML/CFT related issues by sectors.

Goal	Action
Improve collection and sharing of statistical information on AML/CFT issues.	• Conduct awareness with the AML Committees on the obligation of recording and collecting statistical information on AML/CFT activities. • Develop template with guidelines on the collection of statistical information for AML/CFT. • Establish periodic collection of information (3 to 6 monthly) by the FIU. • Explore technology as an option for improving collecting, sharing and storing statistical information.

Implementation of the National Strategy 2022-2025

26. The FIU shall be responsible for monitoring and assessing the effectiveness of this Strategy as well as reporting the progress on an annual basis to the Council.

27. Whilst the FIU will be the key Agency in implementing and monitoring the Strategy, all key stakeholders shall provide support by ensuring compliance with the Strategy at their respective levels. The success of the Strategy is dependent on a collaborative effort.

28. In implementing this Strategy, the Council shall consider any AML/CFT evaluations or related reports that are published. The Republic will remain alert to global threats which may threaten the Republic's stability and for this reason the Republic will continue to enhance its efforts to counter AML/CFT contravening activities.

29. The five-pillar Strategy is the basis of our continued efforts to prevent, deter, detect and disrupt AML/CFT contravening activities. The Republic will ensure that all stakeholders have a clear understanding of the AML/CFT risks, threats and vulnerabilities and that these are adequately addressed.

30. The Republic has established and will continue to develop strong working relationships with international counterparts to facilitate cooperation in combatting AML/CFT contravening activities. The Strategy will ensure that it accurately reflects and addresses identified AML/CFT risks for Nauru and the efforts to combat those risks.

31. It is the desired goal of the Strategy that the following is achieved at the earliest:
1. Completion of the legislative drafting project – September 2023.
2. Establishment of the AMLGC, AMLOC and the PPP for better collaboration – May-June 2023.
3. AML/CFT Risk Identification – September 2023.
4. Enhanced Border Currency Reporting – June 2023.
5. Implementation of targeted financial sanctions – September 2023.
6. Complete preparations for second ME – July/August 2023.

Policy Effective Date	01.07.22
Policy Review Date	30.06.25
Policy Facilitator	Financial Intelligence Unit

40 FINANCIAL ACTION TASK FORCE RECOMMENDATIONS

International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation

*(**Editorial Notes:** The 40 Financial Action Task Force Recommendations are reproduced in full. The reproduction has been done carefully to simply replicate the original copies issued by Financial Action Task Force. In case there is any inconsistency between this and the principal instrument, the principal instrument prevails. These Recommendations are included in this booklet together with the **Republic of Nauru National Strategy for Anti-Money Laundering and Combatting the Financing of Terrorism 2022-2025** for the purposes of information to all stakeholders on the implementation of this Strategy.)*

A. AML/CFT POLICIES AND COORDINATION

1. Assessing risks and applying a risk-based approach

Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This approach should be an essential foundation to efficient allocation of resources across the anti-money laundering and countering the financing of terrorism (AML/CFT) regime and the implementation of risk-based measures throughout the FATF Recommendations. Where countries identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the FATF Recommendations under certain conditions.

Countries should also identify, assess, and understand the proliferation financing risks for the country. In the context of Recommendation 1, "proliferation financing risk" refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7. Countries should take commensurate action aimed at ensuring that these risks are mitigated effectively, including designating an authority or mechanism to coordinate actions to assess risks, and allocate resources efficiently for this purpose. Where countries identify higher risks, they should ensure that they adequately address such risks. Where countries identify lower risks, they should ensure that the measures applied are commensurate with the level of proliferation financing risk, while still ensuring full implementation of the targeted financial sanctions as required in Recommendation 7.

Countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering, terrorist financing and proliferation financing risks.

2. National cooperation and coordination

Countries should have national AML/CFT/CPF policies, informed by the risks1 identified, which should be regularly reviewed, and should designate an authority or have a coordination or other mechanism that is responsible for such policies.

Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policymaking and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate and exchange information domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. This should include cooperation and coordination between relevant authorities to ensure the compatibility of AML/CFT/CPF requirements with Data Protection and Privacy rules and other similar provisions (e.g. data security/localisation).

B. MONEY LAUNDERING AND CONFISCATION

3. Money laundering offence

Countries should criminalise money laundering on the basis of the Vienna Convention and the Palermo Convention. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences.

4. Confiscation and provisional measures

Countries should adopt measures similar to those set forth in the Vienna Convention, the Palermo Convention, and the Terrorist Financing Convention, including legislative measures, to enable their competent authorities to freeze or seize and confiscate the following, without prejudicing the rights of bona fide third parties: (a) property laundered, (b) proceeds from, or instrumentalities used in or intended for use in money laundering or predicate offences, (c) property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations, or (d) property of corresponding value.

Such measures should include the authority to: (a) identify, trace and evaluate property that is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the country's ability to freeze or seize or recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

Countries should consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction (non-conviction based confiscation), or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.

C. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

5. Terrorist financing offence

Countries should criminalise terrorist financing on the basis of the Terrorist Financing Convention, and should criminalise not only the financing of terrorist acts but also the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts. Countries should ensure that such offences are designated as money laundering predicate offences.

6. Targeted financial sanctions related to terrorism and terrorist financing

Countries should implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001).

7. Targeted financial sanctions related to proliferation

Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.

8. Non-profit organisations

Countries should review the adequacy of laws and regulations that relate to non-profit organisations which the country has identified as being vulnerable to terrorist financing abuse. Countries should apply focused

and proportionate measures, in line with the risk-based approach, to such non-profit organisations to protect them from terrorist financing abuse, including:

a) by terrorist organisations posing as legitimate entities;

b) by exploiting legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset-freezing measures; and

c) by concealing or obscuring the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

D. PREVENTIVE MEASURES

9. Financial institution secrecy laws

Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

Customer Due Diligence and Record-Keeping

10. Customer due diligence

Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.

Financial institutions should be required to undertake customer due diligence (CDD) measures when:

(i) establishing business relations;

(ii) carrying out occasional transactions: (i) above the applicable designated threshold (USD/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;

(iii) there is a suspicion of money laundering or terrorist financing; or

(iv) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The principle that financial institutions should conduct CDD should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or enforceable means.

The CDD measures to be taken are as follows:

a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.

c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should be required to apply each of the CDD measures under (a) to (d) above, but should determine the extent of such measures using a risk-based approach (RBA) in accordance with the Interpretive Notes to this Recommendation and to Recommendation 1.

Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering and terrorist financing risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with the applicable requirements under paragraphs (a) to (d) above (subject to appropriate modification of the extent of the measures on a risk-based approach), it should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, although financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

11. Record-keeping

Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should be required to keep all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licences or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction.

Financial institutions should be required by law to maintain records on transactions and information obtained through the CDD measures.

The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.

Additional Measures for Specific Customers and Activities

12. Politically exposed persons

Financial institutions should be required, in relation to foreign politically exposed persons (PEPs) (whether as customer or beneficial owner), in addition to performing normal customer due diligence measures, to:

a) have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;

b) obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;

c) take reasonable measures to establish the source of wealth and source of funds; and

d) conduct enhanced ongoing monitoring of the business relationship.

Financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organisation. In cases of a higher risk business relationship with such persons, financial institutions should be required to apply the measures referred to in paragraphs (b), (c) and (d).

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

13. Correspondent banking

Financial institutions should be required, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal customer due diligence measures, to:

a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;

b) assess the respondent institution's AML/CFT controls;

c) obtain approval from senior management before establishing new correspondent relationships;

d) clearly understand the respective responsibilities of each institution; and

e) with respect to "payable-through accounts", be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank.

Financial institutions should be prohibited from entering into, or continuing, a correspondent banking relationship with shell banks. Financial institutions should be required to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks.

14. Money or value transfer services

Countries should take measures to ensure that natural or legal persons that provide money or value transfer services (MVTS) are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. Countries should take action to identify natural or legal persons that carry out MVTS without a license or registration, and to apply appropriate sanctions.

Any natural or legal person working as an agent should also be licensed or registered by a competent authority, or the MVTS provider should maintain a current list of its agents accessible by competent authorities in the countries in which the MVTS provider and its agents operate. Countries should take measures to ensure that MVTS providers that use agents include them in their AML/CFT programmes and monitor them for compliance with these programmes.

15. New technologies

Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including

new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

16. Wire transfers

Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.

Countries should ensure that financial institutions monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information, and take appropriate measures.

Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373(2001), relating to the prevention and suppression of terrorism and terrorist financing.

Reliance, Controls and Financial Groups

17. Reliance on third parties

Countries may permit financial institutions to rely on third parties to perform elements (a)-(c) of the CDD measures set out in Recommendation 10 or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for CDD measures remains with the financial institution relying on the third party.

The criteria that should be met are as follows:

a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10.

b) Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

c) The financial institution should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11.

d) When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

When a financial institution relies on a third party that is part of the same financial group, and (i) that group applies CDD and record-keeping requirements, in line with Recommendations 10, 11 and 12, and programmes against money laundering and terrorist financing, in accordance with Recommendation 18; and (ii) where the effective implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority, then relevant competent authorities may consider that the financial institution applies measures under (b) and (c) above through its group programme, and may decide that (d) is not a necessary precondition to reliance when higher country risk is adequately mitigated by the group AML/CFT policies.

18. Internal controls and foreign branches and subsidiaries

Financial institutions should be required to implement programmes against money laundering and terrorist financing. Financial groups should be required to implement group-wide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes.

Financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programmes against money laundering and terrorist financing.

19. Higher-risk countries

Financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks.

Countries should be able to apply appropriate countermeasures when called upon to do so by the FATF. Countries should also be able to apply countermeasures independently of any call by the FATF to do so. Such countermeasures should be effective and proportionate to the risks.

Reporting of Suspicious Transactions

20. Reporting of suspicious transactions

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU).

21. Tipping-off and confidentiality

Financial institutions, their directors, officers and employees should be:

a) protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred; and

b) prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU. These provisions are not intended to inhibit information sharing under Recommendation 18.

Designated Non-Financial Businesses and Professions

22. DNFBPs: customer due diligence

The customer due diligence and record-keeping requirements set out in Recommendations 10, 11, 12, 15, and 17, apply to designated non-financial businesses and professions (DNFBPs) in the following situations:

a) Casinos – when customers engage in financial transactions equal to or above the applicable designated threshold.

b) Real estate agents – when they are involved in transactions for their client concerning the buying and selling of real estate.

c) Dealers in precious metals and dealers in precious stones – when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

d) Lawyers, notaries, other independent legal professionals and accountants – when they prepare for or carry out transactions for their client concerning the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

e) Trust and company service providers – when they prepare for or carry out transactions for a client concerning the following activities:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

23. DNFBPs: Other measures

The requirements set out in Recommendations 18 to 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:

a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in paragraph (d) of Recommendation 22. Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to in paragraph (e) of Recommendation 22.

E. TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS

24. Transparency and beneficial ownership of legal persons

Countries should assess the risks of misuse of legal persons for money laundering or terrorist financing, and take measures to prevent their misuse. Countries should ensure that there is adequate, accurate and up-to-date information on the beneficial ownership and control of legal persons that can be obtained or accessed rapidly and efficiently by competent authorities, through either a register of beneficial ownership or an alternative mechanism. Countries should not permit legal persons to issue new bearer shares or bearer share warrants, and take measures to prevent the misuse of existing bearer shares and bearer share warrants. Countries should take effective measures to ensure that nominee shareholders and directors are not misused for money laundering or terrorist financing. Countries should consider facilitating access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

25. Transparency and beneficial ownership of legal arrangements

Countries should assess the risks of the misuse of legal arrangements for money laundering or terrorist financing and take measures to prevent their misuse. In particular, countries should ensure that there is adequate, accurate and up-to-date information on express trusts and other similar legal arrangements including information on the settlor(s), trustee(s) and beneficiary(ies), that can be obtained or accessed efficiently and in a timely manner by competent authorities. Countries should consider facilitating access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

F. POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES, AND OTHER INSTITUTIONAL MEASURES

Regulation and Supervision

26. Regulation and supervision of financial institutions

Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities or financial supervisors should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a financial institution. Countries should not approve the establishment, or continued operation, of shell banks.

For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes, and which are also relevant to money laundering and terrorist financing, should apply in a similar manner for AML/CFT purposes. This should include applying consolidated group supervision for AML/CFT purposes.

Other financial institutions should be licensed or registered and adequately regulated, and subject to supervision or monitoring for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, where financial institutions provide a service of money or value transfer, or of money or currency changing, they should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements.

27. Powers of supervisors

Supervisors should have adequate powers to supervise or monitor, and ensure compliance by, financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose sanctions, in line with Recommendation 35, for failure to comply with such requirements. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the financial institution's license, where applicable.

28. Regulation and supervision of DNFBPs

Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary AML/CFT measures. At a minimum:

- casinos should be licensed;
- competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, holding a management function in, or being an operator of, a casino; and
- competent authorities should ensure that casinos are effectively supervised for compliance with AML/CFT requirements.

b) Countries should ensure that the other categories of DNFBPs are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. This should be performed on a risk-sensitive basis. This may be performed by (a) a supervisor or (b) by an appropriate self-regulatory body (SRB), provided that such a body can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

The supervisor or SRB should also (a) take the necessary measures to prevent criminals or their associates from being professionally accredited, or holding or being the beneficial owner of a significant or controlling interest or holding a management function, e.g. through evaluating persons on the basis of a "fit and proper" test; and (b) have effective, proportionate, and dissuasive sanctions in line with Recommendation 35 available to deal with failure to comply with AML/CFT requirements.

Operational and Law Enforcement

29. Financial intelligence units

Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.

30. Responsibilities of law enforcement and investigative authorities

Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations within the framework of national AML/CFT policies. At least in all cases related to major proceeds-generating offences, these designated law enforcement authorities should develop a pro-active parallel financial investigation when pursuing money laundering, associated predicate offences and terrorist financing. This should include cases where the associated predicate offence occurs outside their jurisdictions. Countries should ensure that competent authorities have responsibility for expeditiously identifying, tracing and initiating actions to freeze and seize property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime. Countries should also make use, when necessary, of permanent or temporary multi-disciplinary groups specialised in financial or asset investigations. Countries should ensure that, when necessary, cooperative investigations with appropriate competent authorities in other countries take place.

31. Powers of law enforcement and investigative authorities

When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to obtain access to all necessary documents and information for use in

those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions, DNFBPs and other natural or legal persons, for the search of persons and premises, for taking witness statements, and for the seizure and obtaining of evidence.

Countries should ensure that competent authorities conducting investigations are able to use a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offences and terrorist financing. These investigative techniques include: undercover operations, intercepting communications, accessing computer systems and controlled delivery. In addition, countries should have effective mechanisms in place to identify, in a timely manner, whether natural or legal persons hold or control accounts. They should also have mechanisms to ensure that competent authorities have a process to identify assets without prior notification to the owner. When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to ask for all relevant information held by the FIU.

32. Cash couriers

Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including through a declaration system and/or disclosure system.

Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing, money laundering or predicate offences, or that are falsely declared or disclosed.

Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing, money laundering or predicate offences, countries should also adopt measures, including legislative ones consistent with Recommendation 4, which would enable the confiscation of such currency or instruments.

General Requirements

33. Statistics

Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems. This should include statistics on the STRs received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for cooperation.

34. Guidance and feedback

The competent authorities, supervisors and SRBs should establish guidelines, and provide feedback, which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and, in particular, in detecting and reporting suspicious transactions.

Sanctions

35. Sanctions

Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with natural or legal persons covered by Recommendations 6, and 8 to 23, that fail to comply with AML/CFT requirements. Sanctions should be applicable not only to financial institutions and DNFBPs, but also to their directors and senior management.

International Cooperation

36. International instruments

Countries should take immediate steps to become party to and implement fully the Vienna Convention, 1988; the Palermo Convention, 2000; the United Nations Convention against Corruption, 2003; and the Terrorist Financing Convention, 1999. Where applicable, countries are also encouraged to ratify and implement other relevant international conventions, such as the Council of Europe Convention on Cybercrime, 2001; the Inter-American Convention against Terrorism, 2002; and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, 2005.

37. Mutual legal assistance

Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions, and related proceedings. Countries should have an adequate legal basis for providing assistance and, where appropriate, should have in place treaties, arrangements or other mechanisms to enhance cooperation. In particular, countries should:

a) Not prohibit, or place unreasonable or unduly restrictive conditions on, the provision of mutual legal assistance.

b) Ensure that they have clear and efficient processes for the timely prioritisation and execution of mutual legal assistance requests. Countries should use a central authority, or another established official mechanism, for effective transmission and execution of requests. To monitor progress on requests, a case management system should be maintained.

c) Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.

d) Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions or DNFBPs to maintain secrecy or confidentiality (except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies).

e) Maintain the confidentiality of mutual legal assistance requests they receive and the information contained in them, subject to fundamental principles of domestic law, in order to protect the integrity of the investigation or inquiry. If the requested country cannot comply with the requirement of confidentiality, it should promptly inform the requesting country.

Countries should render mutual legal assistance, notwithstanding the absence of dual criminality, if the assistance does not involve coercive actions. Countries should consider adopting such measures as may be necessary to enable them to provide a wide scope of assistance in the absence of dual criminality.

Where dual criminality is required for mutual legal assistance, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

Countries should ensure that, of the powers and investigative techniques required under Recommendation 31, and any other powers and investigative techniques available to their competent authorities:

a) all those relating to the production, search and seizure of information, documents or evidence (including financial records) from financial institutions or other persons, and the taking of witness statements; and

b) a broad range of other powers and investigative techniques;

are also available for use in response to requests for mutual legal assistance, and, if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

Countries should, when making mutual legal assistance requests, make best efforts to provide complete factual and legal information that will allow for timely and efficient execution of requests, including any need for urgency, and should send requests using expeditious means. Countries should, before sending requests, make best efforts to ascertain the legal requirements and formalities to obtain assistance.

The authorities responsible for mutual legal assistance (e.g. a Central Authority) should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

38. Mutual legal assistance: freezing and confiscation

Countries should ensure that they have the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered; proceeds from money laundering, predicate offences and terrorist financing; instrumentalities used in, or intended for use in, the commission of these offences; or property of corresponding value. This authority should include being able to respond to requests made on the basis of non-conviction-based confiscation proceedings and related provisional measures, unless this is inconsistent with fundamental principles of their domestic law. Countries should also have effective mechanisms for managing such property, instrumentalities or property of corresponding value, and arrangements for coordinating seizure and confiscation proceedings, which should include the sharing of confiscated assets.

39. Extradition

Countries should constructively and effectively execute extradition requests in relation to money laundering and terrorist financing, without undue delay. Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations. In particular, countries should:

a) ensure money laundering and terrorist financing are extraditable offences;

b) ensure that they have clear and efficient processes for the timely execution of extradition requests including prioritisation where appropriate. To monitor progress of requests a case management system should be maintained;

c) not place unreasonable or unduly restrictive conditions on the execution of requests; and

d) ensure they have an adequate legal framework for extradition.

Each country should either extradite its own nationals, or, where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case, without undue delay, to its competent authorities for the purpose of prosecution of the offences set forth in the request. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

Where dual criminality is required for extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

Consistent with fundamental principles of domestic law, countries should have simplified extradition mechanisms, such as allowing direct transmission of requests for provisional arrests between appropriate authorities, extraditing persons based only on warrants of arrests or judgments, or introducing a simplified extradition of consenting persons who waive formal extradition proceedings. The authorities responsible for extradition should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

40. Other forms of international cooperation

Countries should ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing. Countries should do so both spontaneously and upon request, and there should be a lawful basis for providing cooperation.

Countries should authorise their competent authorities to use the most efficient means to cooperate. Should a competent authority need bilateral or multilateral agreements or arrangements, such as a Memorandum of Understanding (MOU), these should be negotiated and signed in a timely way with the widest range of foreign counterparts.

Competent authorities should use clear channels or mechanisms for the effective transmission and execution of requests for information or other types of assistance. Competent authorities should have clear and efficient processes for the prioritisation and timely execution of requests, and for safeguarding the information received.


NAOERO
GOD'S WILL FIRST