National Risk Assessment

Money Laundering & Terrorism Financing

Republic of Nauru

2018

Table of Contents

ACRONYMS

AML	Anti-Money Laundering
APG	Asia Pacific Group
APGML	Asia Pacific Group on Money Laundering
BBNA	Bendigo Bank Nauru Agency
BNI	Bearer Negotiable Instruments
CTF	Countering the Financing of Terrorism
DNFBP	Designated Non-Financial Businesses & Professions
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
LEA	Law Enforcement Agency
PEPs	Politically Exposed Persons
POCA	Proceeds of Crime Act
NRA	National Risk Assessment
NRO	Nauru Revenue Office
RBA	Risk Based Approach
STRs	Suspicious Transaction Reports
TTRs	Threshold Transaction Reports
WU	Western Union

1.0 BACKGROUND

1.1 Country Context

Nauru's population is approximately 11,500. It had a GDP, in 2017, of approximately AUD203 million[1] and GDP per capita of AUD15,000.

Nauru uses the Australian dollar as its currency and its main sources of foreign income are phosphate exports, fishing licences and approximately 50% of the government budget, of AUD 120-130 million per year, coming from payments from the Australian Government for the Regional Processing Centre. Approximately 35 million per annum is generated by the sale of fishing licences.

Nauru's main export partners are Nigeria 45.5%; Australia 13.7%; Japan 13%; South Korea 11.1%; and NZ 8.7% (2016)

Nauru's imports were estimated to be valued at AUD183.1 million (2013) with the main commodities being food, fuel, manufactures, building materials and machinery. Most of these imports were from Australia (71.9%) with Fiji (8.1%) and Japan 4.4% (2016)[2].

1.2 Government Expenditure

The majority (approx. 37%) of government expenditure is on personal emoluments. Operations cost make up 31% of total expenditure. Operations cost includes purchases, medical supplies and equipment, public works, education, land rental, house rental, recruitment, legal fees and etc.

1.3 Flights

Direct flights link Nauru to Brisbane, Australia; Tarawa, Kiribati; Majuro, Marshall Islands; Pohnpei, FSM; Honiara, Solomon Islands and Nadi, Fiji.

1.4 Shipping

The export of phosphate is continuing, albeit at a lower level and exports of rock to the Marshall Islands are currently underway. Nauru does not have a port capable of accepting large container ships and as such the ships are unloaded by barges.

1.5 Banking and Financial Sector

Nauru has one bank, an agency of Bendigo Bank (an Australian bank) that commenced operations in June 2015. Bendigo Bank Nauru Agency (BBNA) currently holds approximately 9,000 accounts and operates 9 automatic teller machines and there are approximately 7,000 debit/credit cards currently issued linked to these accounts.

EFTPOS is not available on the island however customers can use internet banking, mastercard debit cards and smartphone to make payments.

BBNA offers telegraphic transfers in 16 currencies but not USD, Euro or GBP. BBNA does not offer currency exchange and there is no other (official) currency exchange in Nauru.

BBNA does not conduct transaction monitoring onsite and oversight of transactions is conducted in Australia. BBNA has shown reluctance to report suspicious transactions to the Nauru FIU and instead reports them to AUSTRAC in Australia. It also reports threshold transactions conducted in Nauru to AUSTRAC of which there are more than one per day.

Cash depletion has presented significant difficulties for Bendigo Banks operations on Nauru.

---

[1] https://theodora.com/wfbcurrent/nauru/nauru_economy.html
[2] https://theodora.com/wfbcurrent/nauru/nauru_economy.html

Despite there only being one bank in Nauru, Nauruans and other residents hold bank accounts with other Australian banks that they access through internet banking. Training of bank staff is as per AUSTRAC requirements and is conducted online. Staffs are not currently trained to observe Nauruan legislation.

1.6 Remitter – Western Union

Nauru has one formal remitter, a branch of Western Union. The compliance function for Western Union is done in New Zealand. Western Union operates an unusual model in that total remittances for all customers combined are capped at AUD20,000 per day. Once the daily limit is reached the office closes.

The operator offers an additional alternate remittance operation using the MC business bank account in Australia and internet banking. Funds are accepted in Nauru and transferred out of its MCD account in Australia. In essence, the owner is a one person alternative remittance system. Western Union serves a number of asylum seekers and refugees who are from a range of countries where the risk of terrorist financing is greater.

1.7 Alternative Remittance

There is no firm evidence of alternative remittance occurring on the island, however, the banking behaviour of some of the Chinese business community and some of the refugees show potential red-flags for the operation of alternative remittance services, possibly on an ad-hoc basis.

1.8 Designated Non-Financial Business and Professions

Nauru has two private law firms, no real estate agents, no casinos, no stock market, no bullion dealers or precious stone dealers, no car dealers and no other high-value goods dealers and no insurance companies. Services of the type normally provided by DNFBPs are typically accessed from Australia and paid for from Nauruan-held Australian bank accounts.

1.9 Collection of Taxation

The Nauruan government traditionally did not collect taxation, instead relying on revenue from phosphate extraction to fund the government.

In 2016 it enacted a legislation to commence collection of taxes from businesses based on the rates of tax detailed in the schedule to the Business Tax Act 2016. The Annual Corporate tax rate is 10% of business profit. The first collection commenced in 1 July 2017. A government policy introduced a fuel levy of 40c per litre which applies to private fuel importers.

2.0 OVERVIEW

2.1 Understanding Money Laundering and Terrorism Financing

The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. *Money laundering is the processing of these criminal proceeds to disguise their illegal origin.* This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source.

Money laundering can be broken down into three distinct stages, the Placement state, the Layering stage and the Integration stage.

The **Placement stage** is the initial entry of the proceeds of crime into the financial system. It serves two purposes (1) it relieves the criminal of holding large and bulky cash, and (2) it places money into the financial system.

The **Layering stage** often entails the international movement of the funds. The primary purpose is to separate the illicit money from its source which is done by the sophisticated layering of financial transactions that sever the link with the original crime. Funds are moved from one country to another to elude detection. They exploit loopholes or discrepancies in legislation and take advantage of delays in judicial or police cooperation.

The **Integration stage**, is where the money is returned to the criminal from what seem to be legitimate sources. Having been placed initially as cash and layered through a number of financial transactions, the criminal proceeds are now fully integrated into the financial system and can be used for any purpose.

2.2 NRA Mandate

FATF Recommendation 1 requires jurisdictions to understand money laundering and terrorist financing risks and, where appropriate, coordinate actions domestically to combat money laundering and the financing of terrorism and proliferation. 'Mitigation', in this context is the 'detection and disruption of money laundering and terrorist financing and prevention of proceeds entering the system, and criminals sanctioned and deprived of illicit proceeds'[3].

The ultimate "High Level Objective" of the FATF Recommendations is that:

> *"Financial systems and the broader economy are protected from the threats of money laundering and the financing of terrorism and proliferation, thereby strengthening financial sector integrity and contributing to safety and security"*

2.3 Nauru's Approach

FATF Recommendation 1 has been interpreted by Nauruan authorities to mean that a National Risk Assessment should be undertaken, followed by the implementation of an on-going National Risk Process to ensure that, as prevention and mitigation strategies[4] are implemented, an iterative process is commenced that consistently addresses the (next) highest ML & TF risk.

There are 6 major components to the Nauruan National Risk Assessment process, though not all have been exercised in this iteration of the Risk Assessment. These are:

a) System Mapping,

b) Similar Jurisdiction Analysis,

c) Desk-Based Stress Testing,

d) Interviews of experts and stakeholders,

e) Threat, Vulnerability and Consequence Data Capture, and

f) Systems Testing

The NRA process aims to identify and provide understanding of the following:

1. The scale of laundering through each of the various sectors, products, systems, processes, entities, jurisdictions, etc;

---

[3] Intermediate Outcomes 2 & 3 - http://www.fatf-gafi.org/publications/mutualevaluations/documents/effectiveness.html

[4] Depending on the source, there are a number of methods for addressing (or "controlling") risk, including prevention (or avoidance), mitigation (or reduction), acceptance or contingency planning. In the context of ML/TF risk and the risk-based approach, the most relevant of these methods are prevention (*e.g.*, prohibiting certain products, services, or activities) and risk mitigation (or reduction).
(FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment para 58)

2. How AML/CTF system (laws, processes, procedures etc) is supposed to work compared to how it does work;
3. AML/CTF system effectiveness compared to the various money laundering methodologies that might be attempted;
4. The scale of laundering that remains undetected and why it isn't being detected;
5. The scale of laundering that goes on from foreign predicates either through Nauru or using Nauruan products or services (what vulnerability does Nauru pose in the world's AML/CTF system)
6. The reasons why various ML and TF disruption and prevention processes may not be working.

2.4 Money Laundering Environment, Risks and Vulnerabilities

This Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) NRA has been conducted to assist Nauruan authorities, government and private enterprise to identify, assess, and understand the money laundering and terrorist financing risks for the country, and to take action and apply resources to ensuring such risks are mitigated effectively.

This is the first such assessment and it has identified a range of risks, as well as missing or unavailable data and information that prevent an accurate assessment of all the AML/CTF risks that Nauru faces.

As such this assessment should not be considered the end of this process. It is, in fact, the beginning of an iterative process to address identified risks (commencing with the highest risk), gather data that is currently missing and test mitigation strategies and corrective and preventative actions that have been put in place. This process is expected to continue over many years, with increasing benefits to the Nauruan people from reductions in financially-motivated crime including tax evasion and corruption.

This NRA has been conducted to develop an understanding of how money laundering has occurred in the recent past[5] as well as an understanding of how the Nauruan AML/CTF system is intended to function and predict how it may be circumvented. Consideration has been given to issues that arise from a reliance on suspicious transaction reports and predicate offence data and as such attempts have been made to integrate quantitative historical data with qualitative, predictive information and expert opinion.

The NRA has used the FATF terminology of threat, vulnerability and consequence in describing the money laundering environment currently seen in Nauru. The 'threat' described in this NRA are sources of illicit funds to be laundered; 'vulnerabilities' are the weaknesses in the AML/CTF system that might be exploited. This NRA has ranked relative risks using 'scaled' monetary value (where relevant) to identify the highest risks, as shown by historical information faced by Nauru.
This NRA however has also uncovered the areas where insufficient data exists and where unquantifiable risks exist. Mitigation strategies, corrective and preventative actions have been recommended to fill these gaps and to address the vulnerabilities and risks identified.

2.4.1 Threat

The data and information gathered analysed by Nauruan authorities indicates that the highest risk faced by Nauru is the illegal export of cash (smuggling) which is evident through the compensating cash uplifts as a result of the depleting withholding cash reserve. The highest source of illicit funds is generated by tax evasion followed by corruption and robbery or theft.

[5] Data on predicate and money laundering offences was collated from the past 5 years

2.4.2 Vulnerabilities

The absence of an effective border control measures being applied at the border by the respective law enforcement agencies allows for undetected illegal export of cash.

Internet banking and money transfer facilities are the platforms available and used to remit funds to foreign bank accounts held outside of Nauru, and in particular Australia.

2.4.3 Sectors and Entities

Given that Nauru only has one bank, one remitter and two law firms[6] they are, prima facie, the highest risk entities in Nauru. The NRA process has however uncovered a process of laundering in and through Australia which indicates that the highest risk entities are the commercial banks.

2.4.4 Jurisdictions

Australia is Nauru's greatest vulnerability in terms of a jurisdiction that poses the greatest risk. Nauruans hold bank accounts in other financial institutions in Australia.

2.4.5 Money Laundering Methodologies

Using the FATF methodology, the highest risks faced by Nauru are where the highest threat and vulnerability coincide. An aggregation of this information indicates that the highest risks currently faced by Nauru are depleting cash and the transfer of funds to customer bank accounts held outside of Nauru.

2.5 Data Sources

This NRA is a compilation of information comprised from the detailed, structured analysis of 61 predicate offence cases and 32 STRs; open media source; a desk-based stress-testing process and interviews conducted with officials from the Department of Justice, Office of the Director of Public Prosecutions, Customs, Police, National Revenue Office -Tax, Ministry of Finance, Immigration, and Financial Institutions. Enquiries was also made with other member jurisdictions of the APGML, in respect of money laundering and terrorist financing (on information which they may be aware but that Nauru does not currently have information on) conducted through Nauru; using Nauruan legal entities; or by Nauruans in their jurisdictions.

3.0 WHAT THE DATA SHOWS

3.1 Predicate Offence Information

Reported incidents to Police for the years 2010 to 2018 included a range of predicate offences covering both financially–motivated offences and others. The analysis of predicate offences focussed on the financially-motivated offences such as drugs, fraud, robbery and theft/stealing. The data collected from these predicate offences was extracted to populate the Threat, Vulnerability and Consequence spread sheet. (Details of this analysis process are discussed in this report under section 11-"Methodology")

A total of 94 cases, ranging from 2010 to 2018 were able to be collected which were used to populate the Threat, Vulnerability and Consequence spread sheet. 61 of those cases were provided by Police, 32 were STRs, and 1 was obtained through open media source.

The analysis highlighted a domestic source of all funds to be laundered - no data was available to indicate a foreign source for any of the funds laundered in Nauru[7].

---

[6] Nauru has no real estate agents, no casinos, no stock market, no bullion dealers or precious stone dealers, no car dealers and no other high-value goods dealers and no insurance companies.

[7] A request was made to APG-member jurisdictions seeking information on laundering in or through Nauru or using Nauruan legal entities, or laundering by Nauruans. Only 1 jurisdiction responded with a nil match.

3.2 Vulnerabilities Exploited

Nauru's weak border control system and internet banking and money transfer facilities are the greatest vulnerabilities within the Nauruan AML/CTF system.

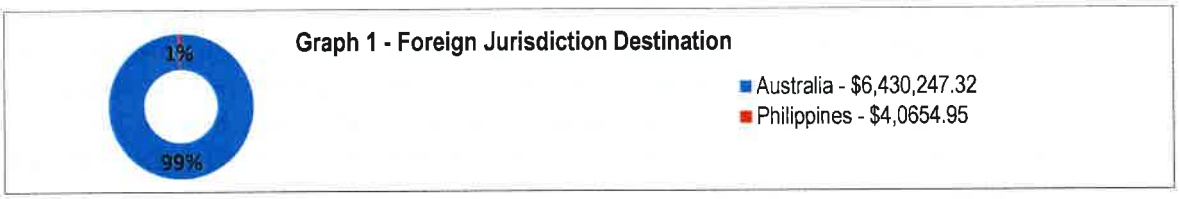
Bank accounts located outside of Nauru are used to transfer funds through over-the counter transactions and internet banking, which is accessible via smartphones. Third parties (persons who don't own either the funds or bank account) also use these foreign bank accounts to deposit or transfer funds. While each customer has a daily threshold (that they choose), there is no limit on the number of transfers a customer may make in a week, month, or a year.

3.3 Sectors and Entities

Given that Nauru only has one bank, one remitter and two law firms[8] they are, prima facie, the highest risk entities (and sectors) in Nauru. The NRA process has however uncovered a process of laundering in and through Australia which indicates that the highest risk entities for Nauru are, in fact, Australian commercial banks. Those banks where funds were moved to, include- Westpac, St George Bank, ANZ Bank, Commonwealth Bank of Australia (in particular the Doncaster branch) and the Bank of China.

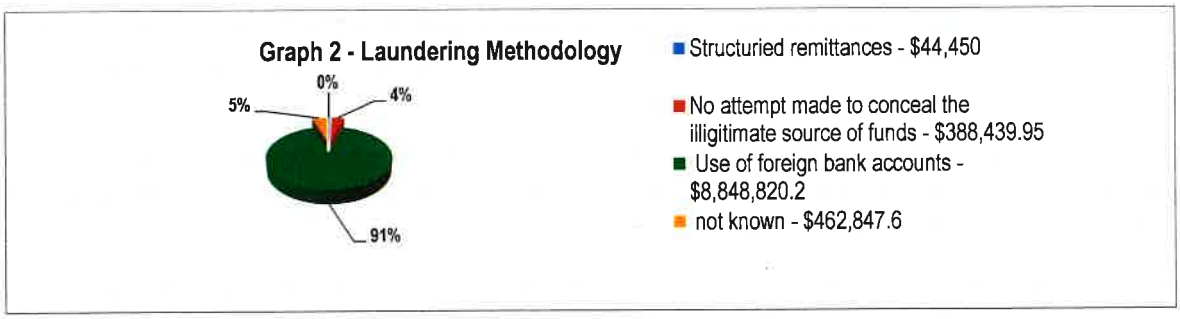
3.4 Jurisdictions

From the information made available, almost all funds generated were transferred to Australia. Data collected and analysed showed that 99% were laundered using internet banking to make transfers from BBNA accounts to other bank accounts held in Australia. The remaining 1% was remitted through Western Union to the Philippines.



3.5 Methods of Laundering

Predicate offence data analysed showed that 91% of these funds were deposited into bank accounts in Nauru and subsequently transferred to bank accounts held in Australia[9]. Less than 1% was moved through structured remittances (Western Union), how 5% was moved was not known while how the rest of the proceeds were moved were either unknown or there were no attempts made to move or conceal the source.

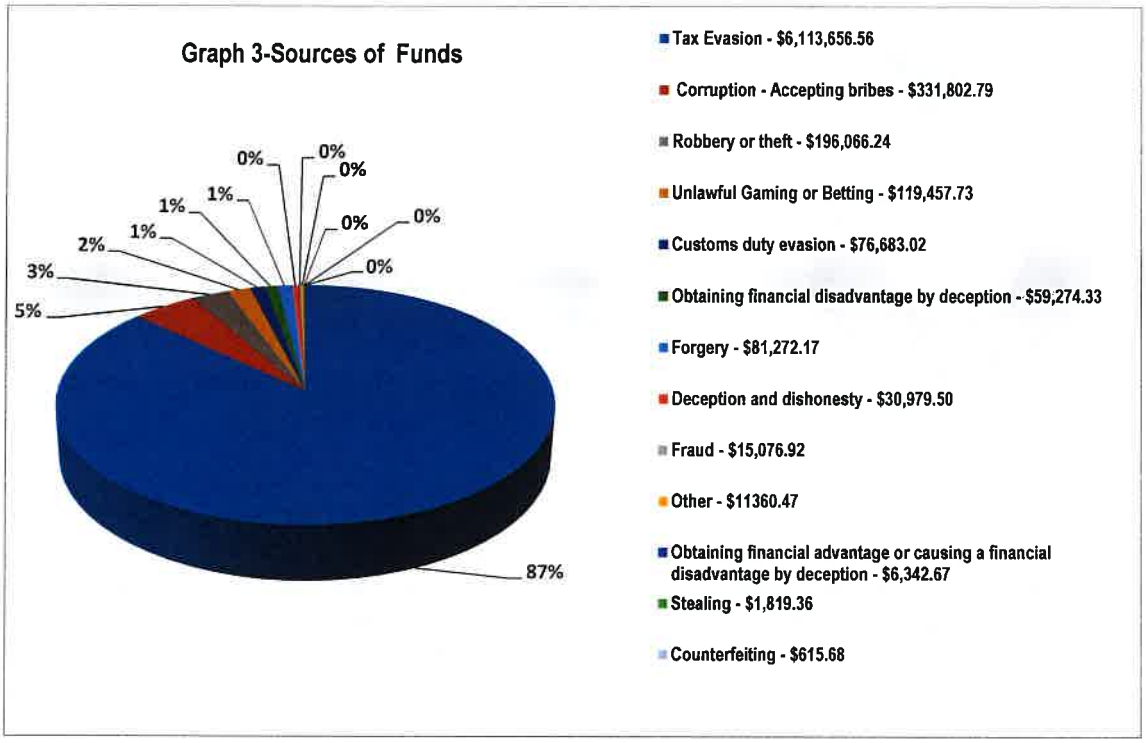


[8] Nauru has no real estate agents, no casinos, no stock market, no bullion dealers or precious stone dealers, no car dealers and other high-value goods dealers and no insurance companies.

[9] Of the 32 STRs filed to FIU, 25 STRs relate to deposits and subsequent transfers. Of these 25 STRs, 20 STRs involved Asian nationals and 5 involved Nauruans who deposited funds in Nauru and immediately transferred them to bank accounts held in Australia.

3.6 Sources of Funds to be Laundered

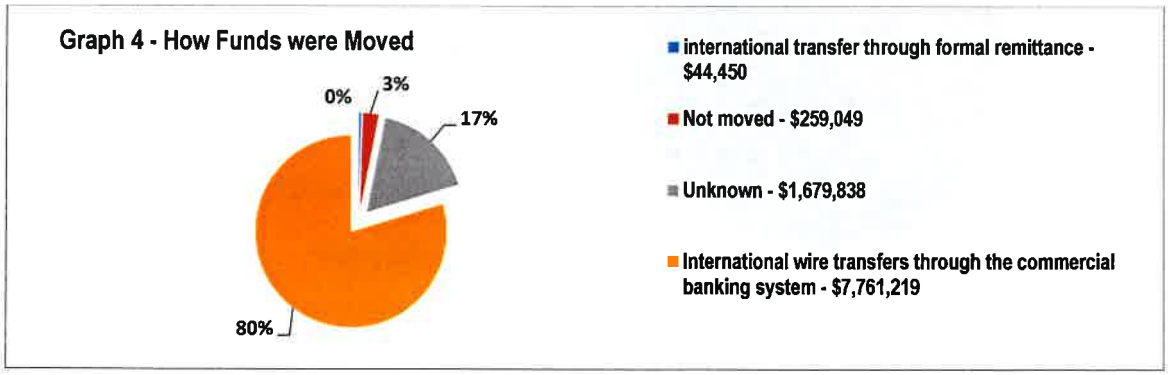
Tax evasion was identified as the main source of funds being laundered within Nauru. Tax evasion made up 87% of funds laundered, compared to 13% shared amongst corruption-accepting bribes; robbery or theft; unlawful gaming or betting, evasion of customs duty; obtaining financial advantage or causing a financial disadvantage by deception and stealing.



3.7 Methods of Moving Funds

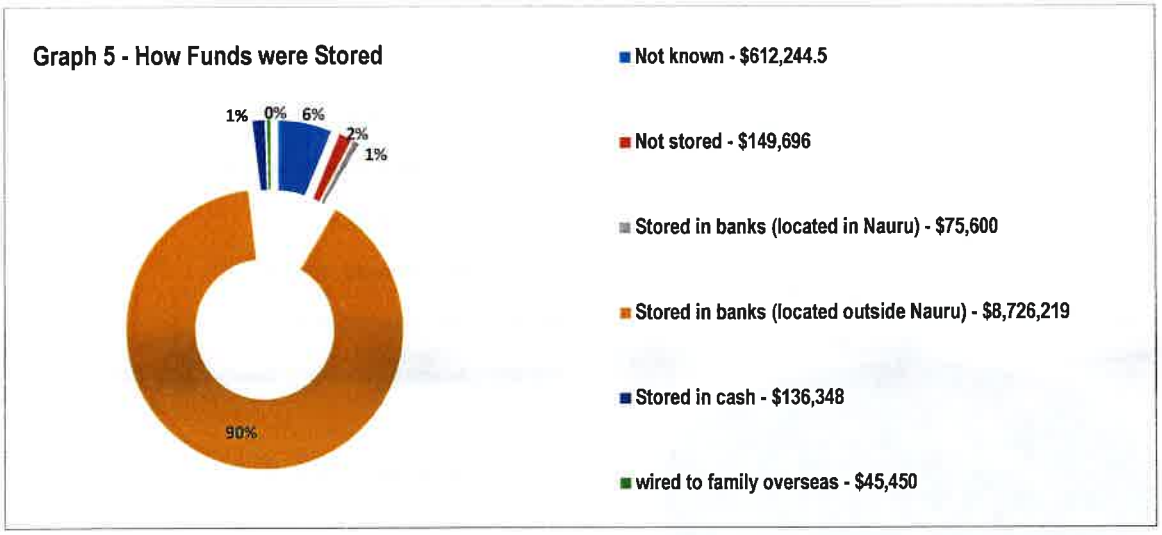
Western Union serves a number of foreign workers as well as refugees and asylum seekers from a number of countries where the risk of terrorist financing is greater. Western Union was used to remit illegally obtained funds (proceeds of fraud) out of Nauru.

While less than 1% of the funds derived were wired to families overseas, how the balance of these funds was moved remain unknown.



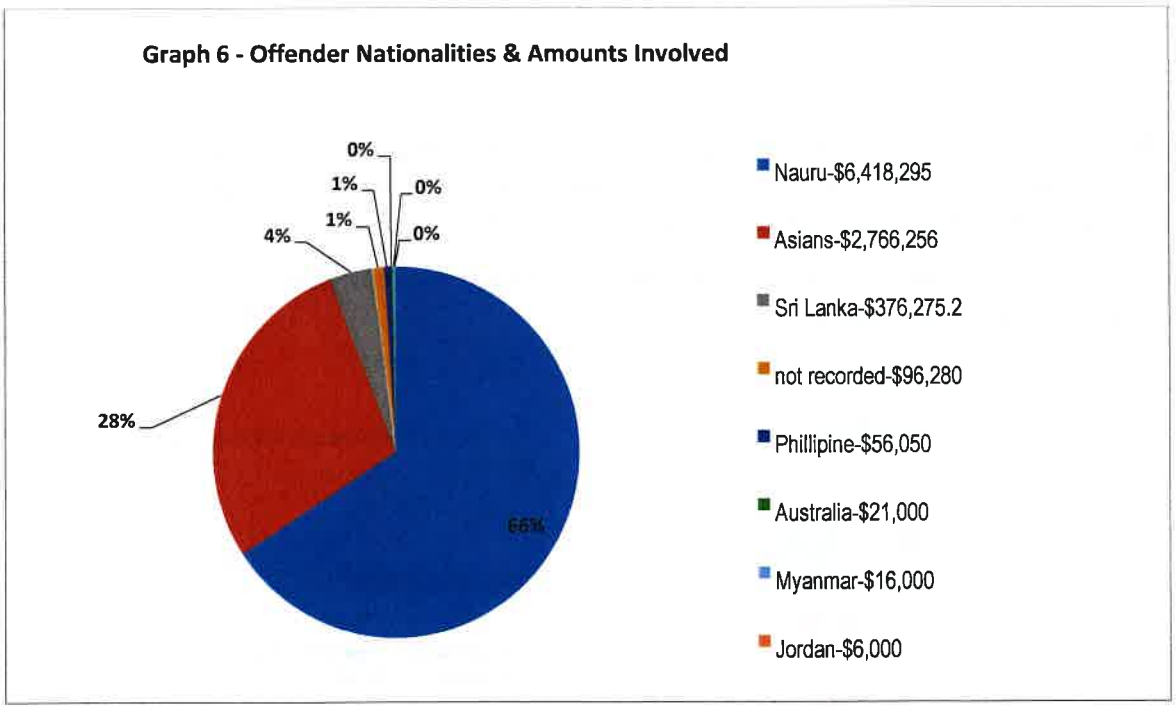
3.8 Methods of Storing Funds

Majority of funds (90%) were stored in banks located outside of Nauru while 2% being kept in the only bank in Nauru. A little fraction of funds were stored in cash while how 6% were stored remain unknown.



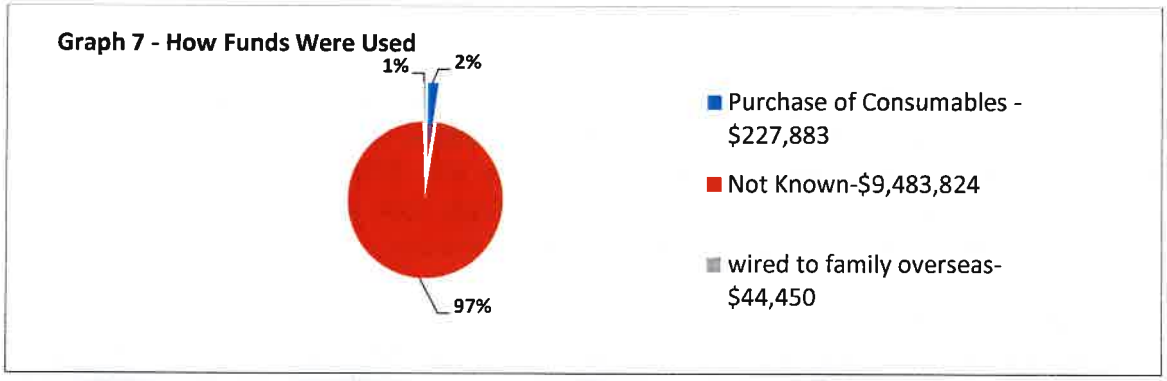
3.9 Current Money Laundering Behaviour

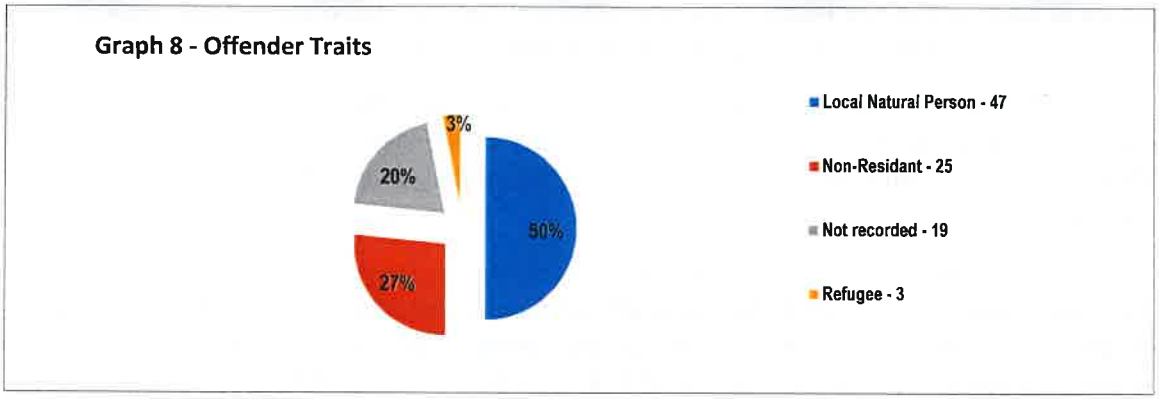
The NRA process has analysed predicate offending and money laundering matters with respect to how the funds involved were laundered. This process has provided detailed information on laundering behaviour. Most offenders are Nauruans (66%) and followed by Asians making up 28%.



3.10 How Funds were Used

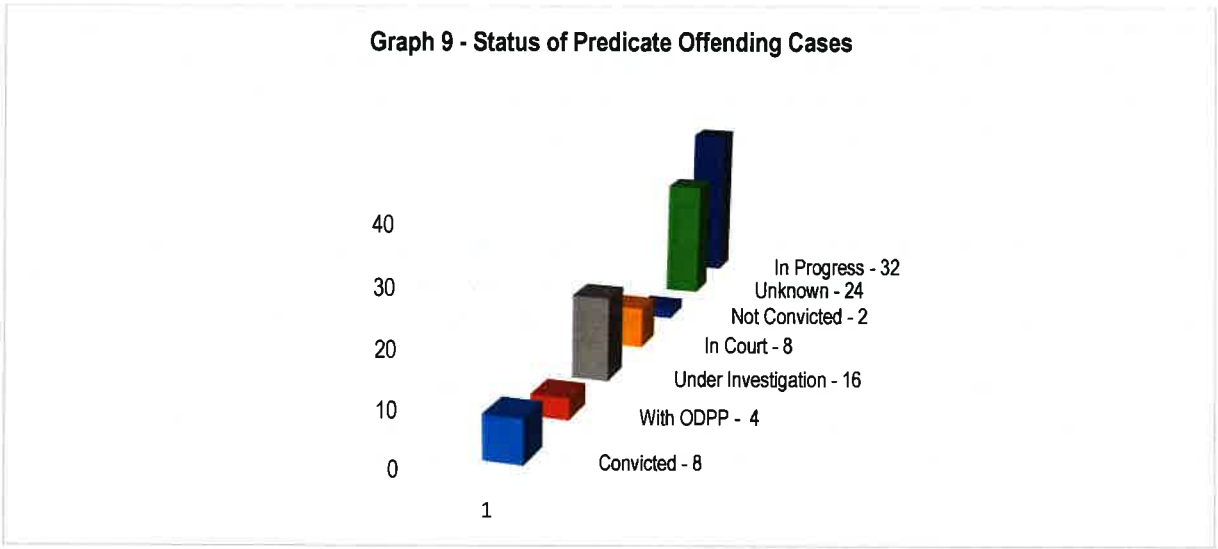
While a very small fraction of funds were wired overseas and some spent on consumable goods, how the majority of 97% or $9,483,824 of these funds were used was not known.





3.11 Disruption, Deterrence and Prevention

Of the predicate offence cases, Police investigations were conducted for 62 cases. Police interviews of suspects and witnesses plus search warrants applied resulted in successfully disrupted cases. As a result, there has been 8 convictions out of the 62 cases while some are either in court, with the Office of the DPP, or still under investigation.



3.12 Qualifications Due to Data Unavailability

As this is the first NRA that Nauru has conducted it has been identified that there are significant gaps in the data available for this process. Provided below are some of the most important types of data that are currently unavailable:

3.12.1 Data on Predicate Offending

Like many jurisdictions undertaking a NRA for the first time, Nauruan authorities have identified that insufficient data is collected by police and prosecutions about the methods of laundering by predicate offenders. This has resulted in a large data gap with 97% of the funds generated by predicate offending being used (or laundered) in a manner that remains unknown. This is a significant data gap for which corrective actions must be put in place.

3.12.2 Illegal Export of Cash

Data on the illegal export of cash is currently unavailable but it is estimated to be in the average of approximately a minimum of $4m in 2017. This has been identified primarily through the high frequency of cash uplifts as a result of the depleting withholding cash reserve. Cash depletion and the lack of documentation suggest that it has been exported legally.

It is suspected, based on the regularity with which cash depletion affects the island, that bulk cash smuggling may actually be one of the primary means of laundering, however, as yet there is insufficient data to support or refute this assertion. This data gap is addressed in the section on 'mitigating strategies'.

3.12.3 Movement of Goods and Assets/Trade-Based Money Laundering

Like many jurisdictions, Nauru does not yet collect data and information on the import and export of goods and services to detect trade-based money laundering. This is an information gap that needs to be filled in order to better understand laundering through this methodology.

Based on the experience of other countries, and the assessments of entities such as the UNODC with respect to the prevalence of trade-based money laundering around the world, trade-based money laundering is suspected of being one of the primary means of laundering however, as yet there is insufficient data to support or refute this assertion. This data gap is addressed in the section on 'mitigating strategies'.

3.12.4 Alternative Remittance

The operator of WU franchise also operates as alternative remitter using the business bank account in Australia and internet banking. It is not known what volume of funds are moved through this method, or if others are also operating in the same way by receiving cash in Nauru and making transfers via the internet from their Australian bank accounts.

3.12.5 System Map

A first draft of the Nauruan AML/CTF System Map is attached to this report. It is not intended to be comprehensive, however it does identify how the various laws, systems and processes are intended to work together to detect, disrupt, deter and prevent money laundering and terrorist financing.

The compilation of this System Map provided several insights into the AML/CTF system and identified gaps in the system which have been included in this first iteration. It is expected that more detailed versions of the system map in future will elicit further insights.

CASE STUDY 1:

Accumulation of suspicious funds in Australian Bank Accounts

Person X, a public servant, landowner and owner of Business A, holding an account with Bendigo Bank, received a number of large cash deposits made by Person A (a third party) in the Business A account in Nauru. Between 10/2/2017 and 14/9/2017 these deposits totalled approximately $518K, and each deposit made into Person X's bank account was immediately followed by an internet banking transfer to a bank account held in Person A's name in Australia. These transfers were described as "salary in respect of business" to Person A, "food items" and others.

Person Y, a Nauruan citizen who is reportedly unemployed, received large cash deposits totalling approximately $450K between 1/1/2017 and 14/9/2017 into his Bendigo Bank account in Nauru. Immediately following each deposit, internet banking transfers were made to bank accounts held in Australia and in particular to Person A's bank account. The transfers were also described as "salary" and "food items".

Person Z, a Nauruan citizen and labourer, also received large cash deposits totalling approximately $3.7m between 1/1/2017 to 13/9/2017 made by persons unknown. These funds were then transferred to bank accounts held in Australia. The description of transfers included- Business A, Person Y, "car rental", and "food items".

Despite the suspicion of Money Laundering & Tax Evasion offences no investigation has commenced, indicating a significant structural vulnerability in Nauru's AML/CTF system which is potentially failing to disrupt, deter or prevent such offending.

3.13 Nauru's Place in the World – Evidence of Money Laundering in and through Nauru by Foreigners

Analysis of available data does not indicate that Nauru is being used by foreigners to launder illicit funds from offences committed abroad, or fund terrorism. The cessation of tax haven operations by Nauruan authorities in early 2000 significantly reduced the risk posed by Nauru to the rest of the world and this is backed up by the available data.

As part of the NRA process, Nauru sought the assistance of the APGML Secretariat to write to the membership of the APGML, seeking any information that the member jurisdictions may have on money laundering or terrorist financing through Nauru or using Nauruan legal entities. Only 1 jurisdiction responded with a nil result.

3.14 Looking ahead – Results of Predictive Analysis [Systems Mapping and Desk-Based Stress-Testing]

3.14.1 Current AML/CFT System does Not Support Detection, Deterrence and Disruption of AML/CFT Methodologies

Nauruan authorities undertook a pilot process of desk-based stress-testing of the Nauruan AML/CTF system. Using known money laundering and terrorist financing methodologies, authorities tested whether current systems would support detection of these methods. From this it was identified that the Nauruan system, as it is currently configured, would not **detect** the following:

- Trade-based money laundering – since insufficient data is collected on trade in goods and services;
- Bulk-cash smuggling – since searches are not made at ports, and scanning machine at the airport becomes inoperative at times;
- Suspicious transactions moved electronically/repatriating of illicit funds – due to Bendigo bank 's refusal to make these transactions visible to NFIU;
- Importation of high value goods – since there is insufficient supervision of importers and sellers. High value goods purchased or sold with cash remain a concern and an area of insufficient data and information; and
- Use of cash to purchase consumables and make lifestyle purchases.

Desk-based stress-testing also determined that the Nauruan AML/CTF system would not disrupt or deter laundering of the following types:

- Bulk-cash smuggling – since no officers had been authorised to detain or seize cash, as required by the POC Act; amd
- Suspicious transactions moved electronically/repatriating of illicit funds – Filing of TTRs are not required by the AML Act, and Bendigo's preference to file STRs to AUSTRAC rather than NFIU.

Further desk-based stress-testing will be conducted in further rounds of the NRA process with the expectation that this process will uncover further deficiencies in the AML/CTF system.

4.0 SOURCES OF INFORMATION FOR THIS REPORT

4.1 Predicate Offence Information

Reported incidents to Police for the years 2010 to 2018 included a range of predicate offences that included financially–motivated offences such as drugs, fraud, robbery, theft/stealing.

Between 2010 and 2018 there were less than fifty (50) drug cases, fraud and robbery incidents recorded by the Police. Theft/stealing cases recorded in the same period however increased from 100 in 2014 to 350 in 2015; 450 in 2016; 500 in 2017; and 130 from January to April 2018.

A total of 94 financially–motivated offence cases, ranging from 2010 to 2018 were able to be collected which were used to populate the Threat, Vulnerability and Consequence spread sheet. Details of this analysis process are discussed in this report under the section "Methodology"). 61 of those cases were provided by Police, 32 were STRs, and 1 was obtained through open media source.

4.2 Suspicious Transaction Reports (STRs)

A total of 32 Suspicious Transaction Reports (STR) have so far been filed to the FIU. 6 STRs were filed by Bendigo Bank Nauru Agency, the only bank on the island, while 26 were received from Austrac through a spontaneous disclosure to NFIU.

The 26 STRs received from AUSTRAC relate to Nauru customers who conducted deposit transactions in Nauru between 2016 and 2017 which subsequent internet banking transfers were made to other bank accounts held in Australia. (this issue is discussed in this report in the section "Australian Bank Accounts"). These 26 STRs received were reported by Bendigo Bank in Australia to AUSTRAC.

The filing of STRs to another jurisdiction (Australia) and Bendigo Bank's subsequent refusal to comply with the requirement of S.17 of the AML/CTF Act presents a significant issue which NFIU is addressing through a range of work-arounds and other methods (addressed in this report under "Bendigo Bank")

The STR data were also used to populate the Threat, Vulnerability and Consequence Spreadsheet to extract the pertinent data. (Details of this analysis process are discussed in this report under the section "Methodology")

4.3 Threshold Transaction Reports (TTRs)

Transaction Threshold Reports (TTRs) are generated by Bendigo Bank Nauru Agency, however they are submitted to Austrac (through Bendigo Bank, Australia) and not NFIU.

There is no information on TTRs in this risk assessment.

4.4 Media Report

Radio and television broadcasts are provided by the Nauru Media Bureau, which is state-owned and is the only media organisation. Nauru has no daily or independent newspaper. Open source local and international media report were utilised to draw information and data that is relevant to this AML risk assessment. This information was "scaled" to account for uncertainty relating to details of the offending alleged.

4.5 Foreign FIUs

Austrac, through a spontaneous disclosure to NFIU, provided STRs that were contained in their database. These STRs relate to customers who hold Nauruan ID or address and were filed by Bendigo Bank, Australia to Austrac. Fiji FIU also exchanged information relating to a STR with NFIU in response to a request. NFIU is a member of the Association of the Pacific Islands FIU and is also currently negotiating a Letter of Engagement (LEA) with Austrac. The information shared by these FIUs provided useful data used in the methodology applied in analysing threats, vulnerability and consequences.

4.6 High-Value Good Dealers

There are no high-value goods dealers on the island. Cars, boats, jewellery, precious stones and metals etc, are sold (if they are sold domestically) in private sales, not through dealerships. There is no information from high-value goods dealers in this risk assessment.

4.7 Taxation Information

The Tax Office was interviewed during this NRA. Until 2013 the Nauruan government did not raise revenue through taxation. The Nauru Business Tax Act came into force in 2016 and has triggered apparent attempts at evasion since then.

Taxation information forms a limited part of this iteration of the risk assessment and it is believed that future versions will benefit from the expanded amount of information that the Tax Office holds.

4.8 Intelligence Reports

Attempts have been made to access and include intelligence reports from Nauru Police. It is believed that the Australian Federal Police, New Zealand Police, Fiji Police and Solomon Islands police, as well as AUSTRAC, NZFIU, Fiji FIU, and Solomons FIU hold relevant intelligence reports that would be useful. Attempts will be made in future iterations of this report, to obtain and include relevant intelligence reports.

5.0 ISSUES WITH RESPECT TO INFORMATION AVAILABILITY

5.1 Bank not Reporting STRs

BBNA has filed a total of 6 STRs (1 in 2016 and 5 in September 2017). The bank had not reported any further STRs to the FIU. The banks' decision not to file further STRs to FIU emanated from their interpretation of the anti-tipping provision in the Australian AML law.
This means that the only bank operating in Nauru will not report further STRs to FIU or comply with the Nauru AML laws.

BBNA has only on one occasion provided the additional information FIU requested on the first STR filed to the FIU. Although FIU made further requests for information relating to the other 5 STRs, the bank was unable to provide the additional information, quoting the anti-tipping provision in the Australian AML law which restricts them from doing so.

5.2 Customs Information

Nauru Customs were interviewed during this NRA and were able to provide information on the procedures currently in place at the airport and seaport.

Customs noted that data relevant to the NRA is not currently captured.

- Import and export data are yet to be centrally maintained and made accessible online from both Customs office based at the Post Office and the Port.
- Company invoices produced by importers are approved by Customs. Payments to suppliers are made by the importers through the Bendigo Bank Agency. There is not any visibility and control over the amount paid for each invoice approved.

Incidents occurred at the border customs area relating to both air and sea-freight cargoes are sometimes recorded by the various duty officers but not centrally recorded and stored. Some of the recorded incidents include:

Airfreight goods: Contraband goods, traditional Kiribati smoke/tobacco were some of the items received through airfreight cargoes; packaged goods sent through the postal services were released to the consignee without the required customs clearance (goods include perfume, gadgets, spices, food products, cigarettes). On one occasion, the supposedly food products turned out to be marijuana seeds; two recorded incidences of dried tobacco leaves with an approximate total weight of 5kg were rolled in aluminium foil (5cm-6cm in length) and packed in empty noodle packets, then placed in a carton. An Irish cake (tobacco product) was placed inside a package of seafood which was detected in an incoming flight from Kiribati - one involved a nun who tried to smuggle in the illegal tobacco packed in the noodle packets. These tobaccos are contrabands. Marijuana from Solomon Islands was sealed in biscuit packets-seemed to be professionally packaged under the guise of biscuits. In 2016, 1kg dried marijuana leaves arrived in one of the incoming flights from Solomon

Islander

Island, the carrier was a Nauruan and dealer, a Solomon islander. The dried leaves were covered in sticky tapes and placed underneath biscuits sealed in a 10kg biscuit bucket.

Sea-freight cargos/goods: Reported case of cigarettes smuggled into Nauru by vessel crews. Cigarettes have also been smuggled through from Vietnam which did not meet the health standard requirement. Though these cigarettes were buried, they were reportedly removed by some members of the public and were assumed to be either consumed or sold. Customs have faced situations where imported goods stored in containers were removed (in the night) from the wharf area before the goods were cleared. Most of these goods include alcohol and food items.

DHL - Three cartons of cigarettes were taken forcefully from the only courier service provider by the consignee without paying duty.

5.3 Additional Sources of Information Required

5.3.1 Predicate Offending Information

Predicate offending information gathered by Nauru Police includes the case number (identifier), date of the offence, source of information, reliability of the information, predicate money laundering offence, and financial institutions that were involved.

Some but not ALL cases included: duration of the predicate offence or event (in months), amount of money involved, local geographic location source, where the predicate offending occurred, method of moving funds, destination jurisdiction, transited foreign jurisdiction, reasons for unsuccessful detection, reasons for unsuccessful disruption, investigating techniques used or attempted, status of the case and some of the offender details such as offender nationality, offender traits, offender age-group and offender occupation.

However, information such as the duration of offence, how the Illicit funds or assets were used or applied, how they were stored and status of such cases were not recorded.

5.3.2 Threshold Transaction Data

Systems Mapping and Desk-Based Stress-Testing indicate that the lack of TTRs is a significant vulnerability in the AML/CTF system.

Filing of TTRs by financial institutions to NFIU is not currently covered under Nauru's legislation. TTRs would have provided some valuable information should they have been made available to FIU. The System Mapping and Desk-based Stress-Testing identified a vulnerability due to a lack of TTRs. This issue is further addressed in the section on System Mapping and Desk-based Stress-Testing.

5.3.3 Border Currency Reporting

A person who leaves or arrives into Nauru with more than $10,000 in cash or NBI is required to declare it to a customs officer. While this is mandatory, a fully completed border currency report has never been filed to Customs by any traveller. This may not necessarily indicate that no cash of more than $10,000 has been taken out of the country, as cash depletion experiences suggest otherwise.

Systems Mapping and Desk-Based Stress-Testing identified that the legislation requires the Minister to designate authorised officers in order to be able to search for and restrain unreported and suspicious cash at the border. No officers have yet been designated. Furthermore, the forwarding of border currency reports to the FIU is yet to be included in a Standard Operating Procedures by Customs.

5.3.4 Import/Export Data

The Systems Mapping and Desk-Based Stress-Testing indicate that the lack of import/export data is a vulnerability with respect to trade-based money laundering.

5.3.5 Foreign Banking Information

Many Nauruans hold bank accounts in Australia which they access through internet banking and debit and credit cards. Media reports and other information suggest that money laundering offences have been committed using bank accounts in Australia. Nauruan authorities have no visibility over these accounts and limited capacity to seek information on them.

5.3.6 Debit Credit Card

The use of debit and credit cards in Nauru, linked to bank accounts held in Australia, is a potential means of repatriating illicit funds. NFIU has no visibility over these transactions as there is no legislative requirement for vendors to report threshold transactions, international fund transfers, etc linked to debit and credit cards.

5.3.7 Use of Proceeds

The fact that the ultimate use of the 97% of the proceeds of predicate offending cannot be determined, it leaves a large gap in authorities' understanding of money laundering behaviour, potential motivations for predicate offending and development of methods of disruption and deterrence.

5.4 Legislative Changes Required regarding Information Sources

5.4.1 Threshold Transaction Data

Nauru should consider amending the AML Act to include the requirement for the bank, the remitter, alternative remitters, and shops to report threshold cash transactions, international funds transfers and debit/credit card transactions.

5.4.2 Import/Export Data

Nauru should consider amending the AML Act to include the reporting of import/export data to the FIU by Customs and other relevant agencies.

6.0 DOMESTIC PREDICATE OFFENDING CONTEXT

6.1 Laundering of Foreign Proceeds: Threat Posed by Nauru to Other Jurisdictions

Outbound remittances through western union places a daily limit at $20,000 while incoming daily remittances averages at 2.5% of the outbound threshold.

Laundering occurs outside of Nauru, given that Nauruans hold bank accounts in Australia and having internet banking access to those bank accounts. In late 2017, Bendigo Bank Nauru Agency customers were given access that allows them to conduct a telegraphic transfer in 16 currencies but not USD, Euro and GBP. There is no visibility of these transactions from Nauru.

7.0 RECOMMENDATIONS – Corrective Actions & Mitigating Strategies

This first iteration of the NRA process has developed a range of corrective actions and mitigation strategies. 'Corrective actions' are intended to address known deficiencies in data availability and identified missing processes that are required if legislation is to have effect. 'Mitigation strategies' are intended to reduce inherent risks that have been identified.

7.1 Illegal Export of Cash and Border Currency Searches

Given the frequent recurrence of cash depletion, there is reason to suspect that bulk cash smuggling may be in the vicinity of approximately a minimum $4m per year.

This issue has remained unaddressed for a number of reasons.

Subsection 96(3) of the POCA permits an authorised officer to examine the luggage or any article carried by any passenger entering or leaving Nauru. If the officer has reasonable grounds to suspect that the passenger is in possession of an undeclared amount exceeding AUD10,000, they may physically search the passenger.

7.1.1 Border Control Procedures

An effective border control procedures should be put in place. This requires;

- A Standard Operating Procedure (SOP) that clearly defines processes/procedures and the different roles of each relevant law enforcement agencies (Customs, Police and Immigration) responsible for the border needs to be put in place.
- The SOP should include currency reporting, search, seizure, detention and its release as covered in Part 6 of the Proceeds of Crime Act (POCA) 2004.
- Training on the application of the SOP should be provided to these agencies (Customs, Police and Immigration).
- Border currency reports to be shared with FIU.
- Travellers who wish to carry cash (threshold to be approved), approval must be granted by the relevant government authority. The approving authority should share this information (applicant/traveller details, approved amount, etc.) with the border law enforcement agencies and FIU.

7.1.2 Customs Proclamation No.2 (1999)

The disclosure for cross border movement of currency is based on overlapping legal provisions. These are set out in the POCA 2004, the Customs Act and Customs Proclamation No 2 1999. Where a passenger fails to declare AUD10, 000 in cash or NBI, Section 96(1) of the POCA provides sanction and defines the penalty. The Customs Proclamation No 2, makes it an offence to carry AUD 2500 out of Nauru unless clearance is given by Bank of Nauru. The penalty is prescribed in the Criminal Code.

The Bank of Nauru no longer exist, therefore the export of cash above the $2,500 threshold covered under the above legislation needs to be reviewed.

7.1.3 Designation of "Authorised Officers"

An 'authorised officer' who is to implement the provisions of currency searches of person and luggage at the border (S.96 & S.97 of the POCA) for any suspicion of undeclared cash on BNI must be designated by the Minister.

The NRA uncovered this deficiency and processes have been put in place to commence addressing this deficiency.

7.1.4 Training of Customs Officers in Cash Detection

Nauru Customs should commence training of its officers on cash detection and seizure procedures to reduce the volume of cash that is suspected of being laundered through bulk cash smuggling.

7.1.5 Cash Detection in Australia

Given Nauru uses the Australian dollar as its currency, Nauru authorities should request assistance from Australian authorities (possibly using cash detector dogs) to detect Australian currency arriving from Nauru into Australia.

7.1.6 Comparison of Departure and Arrival Cards

Nauru authorities should commence a process of comparison of departure and arrival cards to determine whether certain passengers may be failing to declare cash on departure from Nauru but declaring it on arrival into other countries.

7.1.7 Investigation of money laundering and AML/CTF Act offences

Nauru authorities should commence a process of investigation of money laundering, AML/CTF Act, and taxation offences in order to address the structural vulnerabilities that have been identified during this NRA that are presented by the failure to disrupt or deter such offending through the prosecution process.

7.2 A Compounding Problem - History of Interference in Border Searches

Interviews held with Customs officers as part of this NRA has highlighted past instances of false declaration of goods by importers. When Customs have attempted to deny the release of these goods to the importer, there have been instances of interference in the process by senior government officials/politicians, and relatives of importers. On some occasions, goods were forcibly removed from the airport baggage area without customs checks and clearances.

- Customs should consider improving its enforcement of the laws and ensure its compliance.

CASE STUDY 2: Fraud and Transferring of Proceeds

Person B, the financial controller of a supermarket, was observed carrying a large amount of cash in his pockets while shopping at the supermarket. Part of person B's duties was the replenishment of cash in the ATM located in the supermarket.

Subsequent investigations established that funds totalling $56,050 were misappropriated by Person B during the ATM replenishment process. Of this amount, a total of $44,450 was remitted through 13 transactions to his family overseas. None of these were reported as STRs, indicating a compliance failure in the AML/CTF system. Additionally these were not detected by the FIU, as it has no access to threshold transaction reports.

Person B was charged with obtaining financial advantage by deception and sentenced to 18 months imprisonment. No money laundering or AML/CTF Act charges were pursued against the intermediaries in the transactions

7.3 Laundering in Australia using Internet Banking

Bendigo Bank Nauru Agency (BBNA) customers also access their bank accounts online and are able to conduct money transfers through internet banking to other bank accounts held outside of Nauru. While each customer's daily cap differs, there are no limits placed on the number of transactions a customer can make in a week, month or in a year. Nauru FIU currently has no visibility of these transactions and, it is possible that they can facilitate offences within Nauru.

- Nauru should amend the AML Law to require Financial Institutions to report threshold transaction reports on international funds transfers;
- Nauru should address the issue of bank impunity and ensure that financial institutions comply with the requirements of the AML Act;
- Nauru should seek threshold transaction including international funds transfer information on accounts held in Australia by Nauruans;

7.4 Suspicious Transaction Reports

Bendigo Bank Agency filed 6 STRs to the FIU in 2017. After September 2017, Bendigo Bank Agency was unable to comply with S.17 of the AML Act, citing Australia's 'offence of tipping off' provision as set out in clause 123 of Australia's Anti-Money Laundering and Counter-Terrorism Financing Act

2006. This Act, according to Bendigo Bank prohibits them from disclosing suspicious transaction information to third parties (other than AUSTRAC), once they have been reported.

7.4.1 STRs Not Being Reported by Bendigo Bank To Nauru FIU

The issue of a bank reporting STRs to a foreign FIU is a matter of concern. The issue of that bank then claiming that it is unable to then report to the local FIU is of greater concern and is clearly in contravention of Nauruan law.

Nauru needs to pursue Bendigo Bank Agency's compliance with the Nauruan AML Laws in a manner that does not jeopardise the capacity of Nauruans to have access to a bank.

7.4.2 STRs Not Being Reported By Bendigo Bank Nauru Agency

Bendigo Bank is currently refusing to comply with Nauruan Legislation as it pertains to STRs. The FIU is constrained from sanctioning the bank as there is the very real potential for the bank to cease operations in Nauru, leaving Nauru once again, without a bank.

Bendigo Bank should comply with the requirements of the AML Act and fulfil its obligation as a financial institution to report STR to FIU. This might be achieved by a process of education and persuasion, potentially with the assistance of AUSTRAC and other stakeholders. If this fails, consideration perhaps should be given to seeking other banks to set up in Nauru, or the Government setting up its own.

7.4.3 STRs Not Being Reported By Western Union

Western Union has yet to file an STR to FIU. WU should recognise that its role is to collect the basic facts necessary to establish that a transaction is suspicious and report the transaction rather than to first investigate the suspicious transaction. WU should file STRs to FIU. FIU will, as a matter of priority, has commenced the process of educating and encouraging WU to comply.

CASE STUDY 3: Unusual Account Activity

Person C maintains bank accounts with Bendigo Bank that received large cash deposits. Within a span of 4 months, a total of $505,930 was deposited into his personal bank account while $354,560 was deposited into his business bank account. Following each deposit the funds were immediately transferred from these bank accounts via EFT to bank accounts held in Australia.

Person D also maintains a Bendigo Bank account in Nauru that has also received large amounts of cash totalling $407,880 deposited into his account over a span of 6 months. These funds were immediately transferred electronically to financial institutions in Australia. Person C and Person D share the same telephone numbers and are suspected to be the same individual operating multiple accounts.

Despite the suspicion of ML & Tax Evasion offences, no investigation has been commenced, indicating vulnerability in the disruption, deterrence and prevention aspects of Nauru's AML system.

7.5 Dissemination of Information to ODPP

The FIU is mandated to receive, analyse suspicious transaction reports and disseminate intelligence to the Office of the Director of Public Prosecutions (ODPP). The framing of the legislation in this

manner has the potential to impede the function of the FIU, as it may possibly be interpreted as precluding the dissemination of intelligence to other agencies.

A number of STRs received are not directly relevant to the prosecution of a criminal offence in Nauru however may be useful for other purposes (such as taxation), or useful to other jurisdictions.

Nauru should commence a process of legislative reform to support the dissemination of STRs to whichever agency, domestic or international, that might be able to make the best use of the information.

7.6 Information Requests and Dissemination of Reports

The FIU should obtain additional and relevant intelligence information from agencies both domestic and foreign, if required for each case analysis. The outcome of the STR analysis should be disseminated to the appropriate agencies for further investigation, and depending on its result escalated to the respective law enforcement agency.

7.7 Information Lacking and/or Required for NRA Purpose

Not all vital data/information needed to support the National Risk Assessment process were collected or maintained by agencies and institutions.

Information that is currently lacking includes some Police predicate offence, the Bendigo Agency customer foreign banking information, threshold transaction reports, import and export data, and border currency reports.

These information need to be maintained by the respective agencies and shared with FIU.

7.7.1 Predicate Information Data

Predicate offence data from Police provided much of the information required, however some offence cases lacked basic but vital information needed to give a clear and better analysis outcome. This data gaps included: how much money was generated, how funds were stored, used, and or moved; the laundering methodology used; the nationalities and age group of offenders; how the cases were detected and disrupted; the investigation technique used and the status of each case.

These data gaps translated to some "unknown" usage of funds (97%)-as per graph 7, and how 17% of funds were moved-as per graph 4.

A process of engagement with Nauru police should commence as a matter of priority to improve the data gathered by police in relation to financially-motivated crime.

7.7.2 Threshold Transaction Reports

This NRA has identified that STRs alone are not an effective means of detecting money laundering and terrorist financing. The reporting to the FIU of transactions over a specified value would contribute significantly to mitigating some of the vulnerabilities in the Nauruan AML/CTF system.

Financial institutions should, in a prescribed form and manner, report to the Unit any transaction of an amount in cash exceeding $10,000 or such other amount as may be prescribed in the course of a single transaction (or its equivalent in foreign currency). The AML Act needs to be amended to include this reporting obligation of any financial institution.

7.7.3 Border Currency Reports

Customs has not shared a border currency report with FIU. Customs confirmed that a border currency report has not ever been filled by any traveller. The absence of currency reports may imply either no traveller has carried cash above $10,000 or the weak systems and procedures prevalent at the border.

This is likely to be a result of poor training and motivation by Customs officials and potentially a lack of Standard Operating Procedures and pro-forma documents. This should be addressed as a matter of priority by the relevant agencies working together.

7.7.4 Information on Trade in Goods and Services to be Collected and Analysed by NFIU

Given the potential for trade-based money laundering Nauruan authorities should amend the AML legislation to require importers and exporters in goods and services to declare information on those activities to the FIU.

Nauru should also consider expanding supervision of importers and sellers of high value goods (where that occurs) to ensure they comply with their reporting obligations under the AML Act.

7.7.5 Identification of Foreign Accounts and Transactions Conducted on Such Accounts

This NRA has identified that laundering is being conducted by Nauruans and other residents of Nauru using foreign bank accounts, most particularly Australia.

It is possible that this could be mitigated through greater co-operation with AUSTRAC in particular, but also other FIUs in countries with a Nauruan diaspora.

It is also possible that this may also be mitigated through declaration by Nauruans of foreign bank accounts held by them to a relevant government agency. Nauruan authorities should commence a process of consultation through the AML/CTF National coordinating body working group to develop legislation to support this process.

Nauruan authorities should seek dialogue with AUSTRAC and other Australian authorities on this as a matter of priority.

7.8 Audit of Thomson-Reuters Accellus Data on Nauru High-Risk Customers

The desk-based stress-testing process conducted as part of this NRA has identified that the means by which Bendigo Bank, as well as banks in Australia, are using to identify Nauruan PEPs and high-risk customers, is through proprietary databases such as World-Check.

A selective audit of the World-Check database, conducted as part of this NRA, identified several deficiencies in the data held on Nauruan PEPs and high-risk customers, indicating a structural vulnerability in the AML/CTF system.

Information on Politically Exposed Persons and other high risk customers from Nauru needs to be updated on the World-Check database. NFIU should collect this information and submit it to World-Check and other proprietary databases and/or make it available in some other manner.

7.9 Engagement with Foreign FIUs

NFIU will continue to pursue membership of the Egmont group of FIUs to support detection of money laundering by Nauruans.

However, given the considerable difficulties many smaller jurisdictions experience in gaining membership of Egmont, Nauru should, in the meantime, seek to significantly expand its range of bilateral agreements with regional FIUs. Given the significant issues with Nauruans conducting their banking relationships with Australian banks, the first priority should be to establish a relationship with AUSTRAC. Given AUSTRAC's continued preference for only signing MOUs with Egmont members, Nauru should seek some form of information sharing relationship that isn't an MOU.

7.10 Laundering Using Debit, Credit and Stored Value Cards

Given the number of accounts held by Nauruans in Australia (and possibly other countries) and the known methodology of using debit and credit cards to repatriate illicit proceeds, Nauruan authorities

should consider including the capture of threshold transactions using debit, credit and stored value cards in the threshold transaction data to be gathered.

8.0 MITIGATION STRATEGIES FOR THE FIRST ITERATION NRA

8.1 Illegal Export of Cash

Cash depletion has been of significant concern and the illicit movement of cash across the border is the major contributing factor.

If undeclared notes are discovered through screening at the border, there is uncertainty of the next step of action. There are no operational procedures to provide any guidelines in dealing and managing this.

- An effective border control measures should be put in place. There needs to be a Standard Operating Procedures (SOP) that clearly defines processes/procedures. The SOP should also define the different roles of each relevant law enforcement agencies (Customs, Police and Immigration) in executing these procedures at the border. This should include currency reporting, search, seizure, detention and its release as covered in Part 6 of the Proceeds of Crime Act (POCA) 2004.
- The law enforcement agencies, Customs, Police and Immigration should be educated/ trained on their different roles in the SOP, its application and their needs to be an coordinated effort amongst each other.
- When approval for cash export is granted, the approving authority should share this information with law enforcement agencies at the border. This provides key information for risk profiling of travellers.
- An 'authorised officer' who is to implement the provisions of currency reporting and suspicious currency movements (Part 6 of POCA) should be designated by the Minister.
- The Customs Proclamation No 2 (1999), makes it an offence to carry AUD 2500 out of Nauru unless clearance is given by Bank of Nauru. The Bank of Nauru no longer exists, therefore this legislation needs to be reviewed and amended.

8.2 Debit Credit Cards Used to Repatriate Funds

NFIU has no visibility over transactions conducted outside of Nauru with the use of debit and credit cards that are linked to bank accounts in Australia.

The BBNA should make this reports available to NFIU through transaction reporting threshold (for transactions above $10,000), suspicious transaction reports if applicable and if additional information is required by NFIU.

8.3 Accounts Held in Foreign Jurisdictions

Bank accounts held outside of Nauru by any Nauruan should be disclosed to the relevant Nauru government authority by the account holder.

8.4 Assets Imported

High value goods are imported for private use and can also be put on the market for sale. The ability to purchase these items with cash raises some concern as links to international funding cannot be disqualified. The absence of adequate supervision is a vulnerable factor.

Nauru should consider supervising importers and sellers of high value goods and ensure they comply with their reporting obligations under the AML Act.

8.5 Use of Cash

Nauru should consider developing a data source that would support the detection of laundering using cash generated from predicate offending. Potential sources may be trade stores and shops, as in similar jurisdictions the proceeds of crime are often spent on lifestyle expenses and consumables.

9.0 TERRORIST FINANCING RISK ASSESSMENT

9.1 Terrorist Financing – Evidence, Indicators and Issues

The data currently available to Nauruan authorities does not suggest that Nauru has been a source, transit or destination country for terrorist financing.

Whilst it is recognised that some of the refugees and asylum seekers in Nauru come from regions of the world where civil unrest and terrorism occur, there is no current data to suggest that such people are remitting, receiving or storing funds intended for terrorist purposes.

Nevertheless, Nauruan authorities recognise that certain structural problems (including a lack of threshold transaction data; refusal of Bendigo Bank to report STRs to Nauru FIU and the use of Australian bank accounts accessed remotely from Nauru) means that authorities are lacking sufficient insight into financial behaviour that might pose a risk. Nauruan authorities believe that legislation to require the reporting of threshold transactions will further enhance terrorist financing detection, as will an improvement in Bendigo Bank's compliance with the AML Act.

It is hoped that the on-going engagement by Nauru with APG-member countries may elicit information that is currently unavailable.

As such, the corrective actions and mitigation strategies recommended below have been developed with the consideration in mind that terrorist financing indicators, and therefore detection, may be enhanced by improved data collection.

Given the apparent low risk of terrorist financing, enhancements to disruption strategies have not been considered in this iteration of the NRA.

10.0 TERRORIST FINANCING RISK ASSESMENT

The Nauruan NRA have addressed terrorist financing and proliferation financing in the same manner as the money laundering assessment by using the same stages:

g) System Mapping
h) Similar Jurisdiction Analysis
i) Desk-Based Stress Testing
j) Threat, Vulnerability and Consequence Data Capture
k) Systems Testing

10.1 Other Methods Considered

Nauruan authorities are aware that the World Bank methodology uses a review of quantitative and qualitative information on terrorist acts in the jurisdiction, such as enforcement data, intelligence sources, and terrorism research to assess the threat. The rationale being that the level of the terrorist threat impacts the level of terrorism financing.

Some NRA methodologies identify the direction of movement of terrorist financing funds, as well as their sources and channels.

a. *Directions.* By determining the direction of the funds supports assessment of whether funds are generated in the home jurisdiction but used for terrorist operations elsewhere, or the other way around. Another possibility is that funds simply pass through the jurisdiction.

b. *Sources.* The assessment then turns to the sources of the terrorist funds. Financing may come from legitimate sources (such as non-profit organizations, or import/export businesses) or from criminal activities (such as natural resource theft or drug trafficking).

c. *Channels.* Examination of the channels being used to move terrorist funds using enforcement and intelligence data and an estimate of undetected terrorist funds, based on qualitative indicators.

Nauruan authorities have considered this approach and determined that the analysis must include monetary values in order to allow ranking of risks. Furthermore, the directions, sources and channels, though useful, are insufficient of themselves to support decision-making on the allocation of resources. The Nauruan NRA will use the Threat, Vulnerability and Consequence Database to analyse cases in detail to allow prevention and mitigation strategies to be developed.

11.0 NRA METHODOLOGY USED TO COMPILE THIS REPORT

11.1 Risk-Based Approach Based On Evidence

The FATF recommendations require a risk-based approach (RBA) to AML & CFT. The 4th round of Mutual Evaluations has articulated that, underpinning the RBA, is the necessity for jurisdictions to gather and use evidence on a range of key indicators.

These include:

- Predicate offending behaviour;
- Money laundering behaviour;
- Effectiveness of combating actions, including,
    - Effectiveness of detection processes ;
    - Effectiveness of Disruption processes;
    - Effectiveness of Prevention processes with respect to proceeds entering the system;
- Effectiveness of corrective actions and prevention and mitigation strategies;
- Effectiveness of coordination actions;

In essence this requires an "evidence-based approach" as much as it is a "risk-based approach" since the 4th round of mutual evaluations have shown that it is "evidence" that is required to show that authorities understand money laundering and terrorist financing risks and coordinate actions domestically to combat money laundering and the financing of terrorism and proliferation. Evidence of 'effectiveness' requires the ability to show the outcomes of various policy and regulatory changes.

Nauruan authorities intend to use the results of the NRA process to first and foremost address those elements of money laundering and terrorist financing process that are used to raise, move, store and

use the greatest volume of money and weaknesses in the AML/CTF system that may lead to ML and TF going undetected or unaddressed.

In this regard, the NRA will be a 'Risk and Environment' assessment which attempts to identify the system weaknesses that might lead to money laundering and terrorist financing to not being detected, disrupted, deterred or prevented.

11.2 Scale and Characteristics of ML, Terrorism & Proliferation Financing

The Nauruan NRA assessed the scale and characteristics of ML, TF & PF in monetary terms. This was done through the analysis of predicate offending, money laundering offending and other relevant data, capturing details of various offences and processes including the volume of money involved at each stage.

Using monetary values has several advantages over other NRA methodologies.

i. First and foremost, money provides an absolute and objective measure of ML & TF, which avoids the issues and problems faced by subjective and relative measures such as "high, medium and low" (which inherently require a comparison to some other thing -presumably other jurisdictions, or some ideal state. For example, to say the scale of money laundering in a jurisdiction is "high" requires a comparison against either another jurisdiction or against the same jurisdiction at another time or another situation.

ii. Monetary value provides an inherent "weighting" for sectors, entities, products, methodologies, vulnerabilities etc. thereby removing the need to apply "best-guess" weightings to sectors and processes (as is done in the World Bank methodology spreadsheet). The use of monetary values, even if imprecise, gives an immediate indicator as to which sectors, entities, methodologies, vulnerabilities are facilitating, moving or storing the greatest amount of money.

iii. The use of a monetary value allows analysis of money laundering and terrorist financing (and ranking of relative risk) down to a level of granularity of individual entities, individual financial products, geographic locations, jurisdictions money laundering methodologies, etc., etc., which is impossible using subjective measures that require "best-guess" weightings and subjective measures such as "high, medium and low" .

iv. It also potentially provides an inherent baseline measure against which to test the effectiveness of policy changes over time.

This approach may be viewed as supporting a 'threat, vulnerability and consequence assessment' all in one. Articulation of the manner in which funds or assets are raised, moved, stored and used is expected to provide sufficient detail on the source of funds, predicate offences, source jurisdictions, vulnerabilities that have been exploited, typologies of laundering and the channels, products, entities and processes that are used, to allow formulation of corrective actions, preventative and mitigating strategies. The "consequence" in this assessment is measured as the monetary volume at each stage[10].

11.3 Threat, Vulnerability and Consequence Compared Together

Some NRA approaches require the designation of sectors, jurisdictions etc. as either a "threat" or a "vulnerability". Analysis, using predicate offence data etc. is then used to assess the level of threat or vulnerability posed by that element.

Nauruan authorities have considered this approach and decided that such an approach may be challenged.

[10] Acknowledging that monetary value may be an imperfect measure of consequence since the harm caused by one type of offence may not be well equated to the money it generates (or in TF, money that it requires or uses)

Recent research has identified the interdependence between threats and vulnerabilities in AML/CTF rendering delineations in a NRA process subject potentially misleading and raising the possibility of flawed conclusions about appropriate corrective actions and mitigation strategies.

For example, a rogue bank such as HSBC, BNP Paribas may constitute both a threat (due to the illicit profits generated from money laundering or sanctions circumvention) as well as a vulnerability (due to the fact that the bank is disinclined to detect, prevent or report suspicious, or criminal, behaviour of its customers). Similarly, a jurisdiction that formulates laws to actively launder proceeds poses a threat to other jurisdictions; however such a situation is not well captured by the definitions used in most NRA models which would typically describe a destination for proceeds as a vulnerability.

Nauruan authorities aim to avoid these pitfalls by analysing threats and vulnerabilities together in the Threat, Vulnerability and Consequence Database. This approach avoids the need to classify any single entity, jurisdiction, sector or product, law, process, oversight, impediment etc as either a threat or a vulnerability and merely describes them as contributing to 'risk'.

11.4 Mapping of the Jurisdiction's AML/CTF Systems

Fundamental to the understanding of Nauru's AML/CTF system is a means by which to understand how the components of the system are intended to fit together. The Nauruan AML/CTF system is a complex interconnected system of laws, policies, procedures and processes. A detailed understanding of the interaction between these elements is required in order to ensure that the system is fit-for-purpose and context appropriate.

A NRA that relies entirely on data and information generated from within the AML/CTF system has the potential to overlook issues that remain undetected. For example, a 'sectorial vulnerabilities' approach using money laundering cases as the basis for the assessment of vulnerabilities arguably can only identify vulnerabilities that have been exploited by ML and TF methodologies that have been detected. These are therefore, the types of cases that the system is already capable of detecting. This raises the potential problem that the NRA will only focus on matters that the jurisdiction's AML system is already set up to be capable of detecting. Nauruan authorities are aware of the need to uncover the "unknown unknowns" and the AML/CTF System Map is the first stage in that process.

11.5 Desk-Based Stress Testing of the AML/CTF System

Desk-based Stress Testing is the process of conducting simulated laundering in the Nauruan context to identify weaknesses in the Nauruan AML/CTF system. Smurfing, for example, may go undetected in a system that does not require identification of customers making third-party deposits and which do not test financial institution capacity and willingness to report.

Suspected predicate offending for which there is no currently known ML methodology - and which is apparently undetected[11] may be identified through prevention and mitigation strategies developed from Desk-Based Stress Testing.

11.6 Predicate Offence Data (Including Monetary Value of Illicit Funds or Assets)

Nauruan authorities have considered the approach used in some NRA methodologies of only using prosecution data (and in particular money laundering prosecution data) and have formed the opinion that a singular focus on prosecution data, and in particular money laundering prosecution data brings the risk, that if a matter was not prosecuted, then the information may be overlooked in the assessment.

[11] An example is the analysis of wastewater to identify the volume of illicit drugs being consumed by a population which, when combined with the cost of the drugs, provides an indication of the volume of funds or assets to be laundered.

Overlooking other forms of data and information brings the risk that certain sectors and certain jurisdictions will not be analysed if a case has not come before the courts that affects that sector or jurisdiction[12]. Given the limited number of prosecutions compared to predicate offending cases (in particular ML/TF prosecutions in most jurisdictions), and the many and varied reasons why some matters proceed to prosecution and others don't, the information obtained from prosecution records may not result in an accurate picture of the 'scale and characteristics of proceeds from criminal activities' and has the potential to mislead jurisdictions about ML occurring in and through the jurisdiction.

As an alternative approach Nauruan authorities will include predicate offence information along with a range of other intelligence product, open source information and data (including the value of illicit funds or assets generated) and apply a "discount" to account for the potential uncertainty around certain types and sources of information.

11.7 Vulnerabilities

'Vulnerabilities' may be described as '*weaknesses or gaps in a jurisdiction's defenses against money laundering and terrorist financing*'.

In determining the impact of 'vulnerabilities' on the effectiveness of the jurisdiction's AML/CTF system some NRA methodologies use a combination of sectorial vulnerabilities coupled with vulnerabilities in the national combating ability. This approach recognises the interdependence between threats and vulnerabilities, as well as avoiding problems associated with separating sectoral vulnerabilities and combating ability.

Nauruan authorities are aware that the World Bank, for example, assesses vulnerability ratings for the different sectors (Banking, Securities, Insurance, Remittance, Lawyers etc.) by reference to information collected by the working groups multiplied by a weighting applied to the sector, depending on its importance in the country's economy.

The 'National Money Laundering Combatting Ability' is considered in the Nauruan NRA process within the analysis of data, cases and information in the Threat, Vulnerability and Consequence database. It is considered with reference to "failures of the AML/CTF system to disrupt or deter ML & TF" and is based upon a combination of the World Bank National Combating Abilities and Nauruan-specific vulnerabilities generated from mapping of the AML/CTF system. This approach inherently recognises that 'prosecution-as-deterrence' is not the only viable means of preventing ML & TF and that prevention is often preferable as it is less resource intensive.

Nauruan authorities are aware that the World Bank model applies a pre-determine impact of vulnerabilities in 'combatting ability' that exist in a jurisdiction through hard-coded weightings in formulas in their analysis spread sheets. Nauruan authorities considered this and have formed the opinion that the use of 'monetary value' as provided in the predicate offence case data and other information is a preferable alternative.

Ideally a NRA will lead (among other things) to genuinely new discoveries about how ML and TF is occurring and formulation of new responses. Nauruan authorities are aware that the World Bank offers 22 pre-coded 'vulnerabilities' in its model (detailed below in the section on Vulnerabilities). This approach comes with the potential to limit the consideration of issues outside of the 'vulnerabilities' as offered in the model-thereby constraining the potential for genuine new discoveries and development of unique, context-specific approaches.

[12] This narrow focus is in apparent contrast to the WB NRA approach for the analysis of terrorist financing which encourages the casting of a wide net for relevant information.

The pre-coding of vulnerabilities also contains the implicit assumption that a vulnerability - such as the comprehensiveness of asset forfeiture laws - will automatically and permanently render any jurisdiction's AML system less effective if not corrected (whether or not that vulnerability has actually been exploited). Underlying this is the assumption that there is no way to address ML/TF that does not, for example, rely on prosecution of offenders and the forfeiture of assets.

Nauruan authorities considered this and have formed the opinion that the use of a pre-coded list of vulnerabilities is not the preferred method of analysis and have opted to consider those vulnerabilities alongside the analysis of cases in a broader methodology in the Threat, Vulnerability and Consequence Database.

11.8 Analysis of Other Jurisdictions

Nauruan authorities are cognisant of the risk of feedback loops caused by relying (only) on data provided from within a system to assess that system's effectiveness.

The sources of information for some jurisdiction's NRAs have been almost exclusively domestic with the experts providing opinion drawn locally and the data examined sourced domestically. Such an approach comes with an inherent risk that if a particular type of ML has not been detected (perhaps because the data is not being collected or reported or the local institutions and authorities have no experience of it) there may be no data indicators that it is occurring. In this instance there is a risk that the NRA may not result in the identification of weaknesses in the system caused by data gaps, legislative gaps, process gaps or some other vulnerability, or a threat that has never been considered.

Nauruan authorities aim to avoid this problem by actively analysing the methods of ML & TF detected in similar jurisdictions in order to thereby provide data for the Desk-Based Stress Test conducted on the AML/CTF System Map determine whether Nauruan systems would detect, deter or prevent such methods.

11.9 'Consequence' – as Measured Using Money

Some NRA methodologies attempt to combine information from the analysis of the 'scale and characteristics' with the information on 'sectorial vulnerabilities' and 'national combating ability' to arrive at an overall money laundering risk.

Nauruan authorities have considered this approach and have formed the opinion that this concept of 'risk' is truncated, as it ignores 'consequence' which is an inherent aspect of most concepts of risk. Assessment of the effective exploitation of vulnerabilities on monetary terms – ie which sector, entity, product, process etc. was most effectively exploited by money launderers.

A 'consequence' may be implied through the use of a monetary figure, thereby providing an objective measure of risk and an available guidance on where resources might be best applied in Nauru to counter the greatest volume of laundering[13]. The formulation of corrective actions and prevention and mitigation strategies should be focussed toward the vulnerabilities that give rise to the ML methods that are used to move the greatest value of illicit assets or funds.

This may be viewed as including the 'financial consequence' in the risk analysis and could be achieved by a 'scale and characteristics' analysis that quantifies the scale of laundering in monetary

[13] An alternate concept of 'risk' if this were a useful approach may be to identify the 'threat' as the volume of funds and assets available to be laundered; the vulnerabilities as the weaknesses in the system that may be exploited; and the 'consequence' as the volume of funds that were actually laundered.

terms and addresses vulnerabilities that are identified as having been exploited to the greatest monetary extent.

11.10 Articulation of the Results of the NRA

Nauruan authorities aim, at the end of the first round of the NRA process to be able to articulate the precise means in which money laundering and terrorist financing are occurring in Nauru, and relating to Nauruans, to a level of detail that goes down to (among other things) individual sectors, entities, products, geographic locations, types of offenders, and money laundering methodologies.

This approach breaks down the amount of funds/assets laundered into the various sectors, methods, entities, processes, vulnerabilities exploited etc. to ensure that the Nauruan authorities, agencies and stakeholders have a broad understanding of how illicit funds are laundered. This approach potentially leads to the recognition that any one ML methodology may be remedied by a range of alternate actions and/or that behaviour modification may require many changes across a range of AML system elements - agencies, laws, entities etc.

Systemic weaknesses or vulnerabilities that have not been exploited but which are shown by the Desk-Based Stress Testing, as being open to exploitation, may require a different approach, as the volume of funds estimation is be based on less robust information.

11.11 Combating ability Vulnerabilities'

Nauruan authorities are aware that some NRA approaches assess the national combating ability through an assessment based on pre-determined variables which are then assessed by expert working groups. These variables attempt to capture the high level factors in the country such as the quality of the judicial processes, the effectiveness of the law enforcement, domestic and international cooperation. The ratings given to these input variables by the assessors in the Working Groups, as well as the built-in assumptions and properties of the tool such as weights and pre-conditions all together generate an overall score for national combating ability.

The threat, vulnerability and consequence database considers the following potential vulnerabilities.

- Quality of AML Policy and Strategy
- Effectiveness of ML Crime Definition
- Comprehensiveness of Asset Forfeiture Laws
- Quality of FIU Intelligence Gathering and Processing
- Capacity and Resources for Financial Crime Investigations (incl. AF)
- Integrity and Independence of Financial Crime Investigators (incl. AF)
- Capacity and Resources for Financial Crime Prosecutions (incl. AF)
- Integrity and Independence of Financial Crime Prosecutors (incl. AF)
- Capacity and Resources for Judicial Processes (incl. AF)
- Integrity and Independence of Judges (incl. AF)
- Quality of Border Controls
- Comprehensiveness of Customs Regime on Cash and Similar Instruments
- Effectiveness of Customs
- Controls on Cash and Similar Instruments
- Effectiveness of Domestic Cooperation
- Effectiveness of International Cooperation
- Formalization Level of Economy
- Level of Financial Integrity
- Effectiveness of Tax Enforcement
- Availability of Independent Audit
- Availability of Reliable Identification Infrastructure

- Availability of Independent Information Sources
- Availability and Access to Beneficial Ownership Information
- Effectiveness (courage, experience and professionalism) of financial crimes investigator and investigatory bodies;
- Effectiveness (courage, experience and professionalism) of Financial Crime Prosecutors and Prosecutorial Bodies;
- Legal precedent favouring a requirement to prove predicate offending in ML prosecution;
- Robustness of the regulatory framework;
- Effectiveness of regulation and aggression of regulators;
- Balance between profit motive and law abidance in the financial and other sectors;
- Level of reliance on financial institutions as the main source of ML detection;
- Potential for non-state actors to bring cases in court (eg Obiang prosecution in France)
- Political will to target foreign proceeds laundered through the jurisdiction;
- Political will to criminally prosecute bankers and other professional launderers;

11.12 Threat Assessment

11.12.1 Predicate Offense-Focused Threat Assessment

The ML 'threat' is generally accepted as being linked directly to the volume of illicit funds or assets generated within the jurisdiction (or sent to the jurisdiction). It might be expected from this that a threat assessment would identify the value of illicit funds and assets generated from domestic offences and illicit remittances.

Nauruan authorities are aware that some NRA methodologies do not do this. The World Bank methodology, for example, in its 'Predicate offense-focused threat assessment' collects data on predicate offences but only collects data on the following elements;

- number of cases detected or investigated ;
- number of cases prosecuted;
- number of persons convicted;
- amount of proceeds seized or frozen;
- amount of proceeds confiscated;

Since the number and the amount of proceeds seized or confiscated are potentially influenced more by the effectiveness of the AML/CTF system – specifically intelligence, investigation and prosecution processes - than the size and nature of the threat, the Nauruan NRA instead used information on the value of proceeds generated, rather than the value of proceeds seized and confiscated, in assessing threats and vulnerabilities.

To achieve this the Nauruan authority approach collected data on the value of illicit funds or assets generated and moved into and out of Nauru – as well as moved in other jurisdictions by Nauruans - emanating from a broad range of offences based on all information available to authorities, not just prosecution data.

11.12.2 Sector-Based Threat Assessment

Nauruan authorities are aware that some NRA methodologies use a 'Sector-based threat assessment' to assess the ML threat experienced by the various sectors.

Nauruan authorities have assessed the 'sectoral threat' through analysis of the value of total illicit funds drawn from the analysis of actual cases/matters and incidents.

Some NRAs apply ratings for each sector of 'high' through to 'low' based on the opinion of experts. Such an approach, while it may be a useful judgement, is inherently a *relative judgement* which by

its nature must be a comparison to some alternative state or metric (ie 'high' compared to what?) Nauruan authorities have assessed that a more appropriate approach will be to base the threat assessment upon monetary values of predicate offences and base the relative assessment of risk between various elements in the AML/CTF system on the specific volume of those illicit funds flowing through each sector and the manner by which those funds have been handled moved and/or stored (indicting the specific elements within those sectors that have been exploited).

Nauruan authorities have also determined that analysis at a sectorial level may be insufficiently granular to support decision making about the allocation of scarce resources and will, over and above the sectorial assessment, assess individual entities within sectors to determine those that pose the greatest risk.

11.12.3 Origin-focused Threat Assessment

Some NRA methodologies include an 'Origin-Focused Threat Assessment' to determine the threat posed by:

- offences committed in home jurisdiction;
- offenses committed in a foreign jurisdiction; and
- offenses committed in both;

Nauruan authorities have considered this approach and determined that this data is captured in the Threat, Vulnerability and Consequence Database but includes monetary value as the objective measure.

11.13 Case-data collection – the Threat, Vulnerability and Consequence Database

The data collected in the Threat Vulnerability and Consequence Database. It's inputs/fields are as follows:

▪ Case number (identifier)	▪ Negligence and complicit
▪ Reference number for AML offence	▪ Amount handled by Institution
▪ STR identifier number (if applicable)	▪ Laundering Methodology
▪ Duration of the AML offence or event (in months)	▪ Amount laundered via method
▪ Date of the offence or event	▪ Financial Product
▪ Source of the information	▪ Amount laundered using product
▪ Reliability of the Information	▪ Asset Type
▪ Offence	▪ Amount laundered through Asset Type
▪ Total Money Generated by All Offences?	▪ Governorate
▪ Macro Analysis effect	▪ Amount Sourced from Governorate
▪ Time-value discount	▪ Governorate
▪ Reliability Discount	▪ Amount laundered in Governorate
▪ Time, Reliability, and Macro-analysis Combined	▪ Source Jurisdiction
▪ Total Money Generated by All Offences (Discounted)	▪ Amount from foreign jurisdiction
▪ Method of Use or Application	▪ Destination Jurisdiction
▪ Monetary value of method Use or Application	▪ Amount going to foreign jurisdiction
▪ Method of Moving the Funds.	▪ Transited foreign Jurisdiction
▪ Monetary value moved via method ?	▪ Amount transiting through a foreign jurisdiction

▪ Intermediary	▪ Nationality Of Offenders
▪ Amount handled by intermediary	▪ Offender Traits
▪ Bank	▪ Offender Age-Group
▪ Negligence and complicit	▪ Offender Occupation
▪ Amount handled by Bank	▪ Method of detection
▪ Institution	▪ Reasons for unsuccessful detection
▪ Negligence and complicit	▪ Reason of unsuccessful disruption
▪ Amount handled by Institution	▪ the status of the Case
▪ Intermediary	▪ Investigation Techniques used or attempted

For each case or matter that is entered into the database the monetary value that was involved is recorded. This monetary value has a discount applied to it to account for the reduced value of information that is less than certain. This "weighted" monetary value is then used to scale each sector, entity, product, methodology, offender traits etc. to provide a detailed understanding of money laundering within and through the country.

11.14 Domestic and International Funds Flows

Some NRA methodology includes and analysis of international funds flows into and out of the jurisdiction. This analysis provides useful data on potential cross-border flow of illicit funds. Later stages of the Nauruan NRA will seek to include an analysis of the flow of funds both internationally and through various sectors of the jurisdiction. An understanding of the volume of funds flowing through the various sectors may provide and enhanced understanding of the threat posed by and to the various sectors.

11.15 Asset/Trade Flows

Trade-based money laundering and some of the more sophisticated ML methodologies use the movement of assets, both tangible and intangible, as opposed to the movement of funds. Later stages of the Nauruan NRA will seek to include data on asset and trade flows.

11.16 Overall Money Laundering Risk Level

Some NRA methodologies attempt to articulate an overall money laundering risk for the jurisdiction.

The 2013 FATF Guidance suggests that the NRA arrive at:

"an overall picture of the national ML/TF risks across the AML/CFT regime", it however, does not require a jurisdiction to articulate an overall money laundering risk level.

Nauruan authorities intend to allocate the greatest resources to whatever the highest risks are. The articulation of a jurisdiction risk level has been considered by Nauruan Authorities and assessed to be unnecessary to understanding and addressing the ML & TF risks facing the country. The main purpose of the NRA is to support decision-making about the allocation of scarce resources to combat ML&TF. The process of addressing risk will be an iterative process, applying resources to each new highest risk as money laundering behaviour evolves. This process is unlikely to be aided by deciding an arbitrary "high, medium or low" level of overall jurisdiction risk, though authorities may attempt to articulate the national scale of money laundering in monetary terms in future NRAs.

11.17 AML/CTF Systems Testing

This current iteration of the NRA has not attempted to test any elements of the AML/CTF System. Future iterations will seek to use a Mystery Shopper process to identify vulnerabilities that may be impossible to identify in other ways.