ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING (AML/CTF) PROGRAM

PART A

TABLE OF CONTENTS

1. DOCUMENT MANAGEMENT INFORMATION 2
2. DEFINITIONS AND INTERPRETATION 3
3. POLICY STATEMENT 4
4. OBJECTIVES 4
5. AML/CTF PROGRAM 4
6. DESIGNATED SERVICES 5
7. SIZE, NATURE & COMPLEXITY 5
8. RISK ASSESSMENT 6
9. RISK MANAGEMENT AND MITIGATION 8
10. ROLES, RESPONSIBILITIES AND RESOURCES 9
11. AML/CTF AWARENESS TRAINING PROGRAM 10
12. STAFF DUE DILIGENCE PROGRAM 10
13. ONGOING CUSTOMER DUE DILIGENCE (OCDD) 11
14. TRANSACTION MONITORING 11
15. ENHANCED CUSTOMER DUE DILIGENCE 12
16. PERIODIC IDENTITY REFRESH 12
17. DOCUMENT RETENTION 13
18. TRANSACTION REPORTING 13
19. AUSTRAC FEEDBACK 14
20. REVIEW 14
21. MONITORING COMPLIANCE 14

Appendix A - Enterprise ML/TF Risk Assessment 15

1. DOCUMENT MANAGEMENT INFORMATION

VERSION	AUTHOR/REVIEWER	REVISION	APPROVAL	DATE OF APPROVAL	NEXT REVIEW DATE
1.0	General Counsel	Original	Board	January 2018	January 2019
2.0	Risk and Compliance Manager	Annual review	Board	February 2019	February 2020
3.0	Risk and Compliance Manager	Annual review	Board	May 2020	May 2021

Document purpose

The purpose of this document is to record Part A of the AML/CTF Program for NAIF which is a standard AML/CTF Program established under section 84 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML/CTF Act**).

2. DEFINITIONS AND INTERPRETATION

The following definitions apply when used in this AML/CTF Program.

ABN	Australian Business Number
ACN	Australian Company Number
ADI	Authorised Deposit-Taking Institution
AML/CTF	Anti-Money Laundering and Counter-Terrorism Financing
AML/CTF Act	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)
AML/CTF Rules	*Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)* (Cth)
APRA	Australian Prudential Regulation Authority
ASIC	Australian Securities and Investments Commission
AUSTRAC	Australian Transaction Reports and Analysis Centre
Beneficial Owner	Has the meaning given in Attachment 1 (Collection and Verification of KYC Information) to Part B of this Program
Customer	The person to whom NAIF provides a designated service
CIP	Customer Identification Process
Declaration	Declaration 2 of 2017 dated [*] 2017 made by the AUSTRAC CEO
ECDD	Enhanced Customer Due Diligence
Export Finance	Export Finance Australia formerly known as Export Finance and Insurance Corporation (Efic)
Execution Team	Refers to those employees involved in NAIF transactions
NAIF	Northern Australian Infrastructure Facility
FATF	Financial Action Task Force
HR	NAIF's Human Resources department
KYC information	Know Your Customer information
ML	Money Laundering
Northern Australia	The area that includes the following: (a) the Northern Territory (b) the areas of Queensland and Western Australia that are North of the Tropic of Capricorn other than the Meekatharra Statistical Area level 2 (c) the areas South of the Tropic of Capricorn of each Statistical Area level 2 that has an area covered by paragraph (b) (d) the following Statistical Areas level 2: (i) Gladstone; (ii) Gladstone Hinterland; (iii) Carnarvon; (e) the Local Government Areas of Meekatharra and Wiluna (despite paragraph (b)) (f) the territorial sea adjacent to areas covered by paragraphs (a) to (d).

PEP	Politically Exposed Person (as defined in the AML/CTF Rules)
Regulator	Any of APRA, AUSTRAC, ASIC or any other applicable Australian Federal or State agency, government or entity authorised to regulate ADIs, NAIF or entities that are subject to AML/CTF legislation
SMR	Suspicious Matter Report
Staff	means all employees of NAIF including full-time and part-time employees, agents, consultants and contractors
TF	Terrorism Financing
TRA	Transaction Risk Assessment

3. POLICY STATEMENT

The NAIF Board and Executive are committed to policies and procedures that help in combating money-laundering and terrorism-financing (**ML/TF**).

Money-laundering (**ML**) refers to engaging in acts designed to conceal or disguise the true origins of criminally-derived proceeds so that they appear to have derived from legitimate origins or constitute legitimate assets.

Terrorism-financing (**TF**) refers to the act of providing financial support to terrorism or terrorist organisations.

NAIF's ML/TF risk management methodology is:

(a) to identify the ML/TF risks for its customer, products and services, delivery channels and countries with which it deals;

(b) to assess the profile of the identified ML/TF risks to determine their nature and severity;

(c) to design controls to manage and mitigate the ML/TF risks it has identified in accordance with their nature and severity; and

(d) reviewed on a regular basis, including to reflect typologies, case studies and other guidance published by AUSTRAC and any changes to the ML/TF risk environment in which NAIF operates (including any actual or potential ML or TF incident involving or facilitated by NAIF's provision of a designated service or identified by NAIF's transaction monitoring program).

NAIF Staff may face disciplinary action if they fail to follow NAIF's AML/CTF procedures. NAIF may terminate the relevant contract or appointment terms of any director, officer or Staff member who is found to have, without reasonable excuse, failed to comply with any of NAIF's AML/CTF related systems, controls or procedures established in accordance with Part A or Part B of this AML/CTF Program.

In addition, individual Staff members may be subject to prosecution and legal action by a third party or the AML/CTF regulator (AUSTRAC), if found to have been concerned in, or involved with, a contravention by NAIF of its obligations under the AML/CTF Act or if found to have contravened any other AML/CTF laws and regulations.

4. OBJECTIVES

The purposes of the AML/CTF Act include to assist Australia in combating ML and TF. The AML/CTF Act applies to reporting entities.

A reporting entity is a person who provides one or more designated service(s). Designated services are specifically defined under section 6 of the AML/CTF Act.

NAIF provides, or intends to provide, some designated services and is therefore a reporting entity for the purposes of the AML/CTF Act.

As a reporting entity NAIF is required to identify, mitigate and manage the risk that it may reasonably face that its provision of designated services might involve or facilitate ML or TF (**ML/TF Risk**), including by reporting certain suspicious matters to AUSTRAC.

5. AML/CTF PROGRAM

The AML/CTF Act requires that reporting entities adopt and maintain an AML/CTF program. Measures included in that program are required to reflect that entity's assessment of its ML/TF Risk.

This AML/CTF program (**Program**) has been tailored to NAIF's ML/TF risk, following a risk assessment undertaken by NAIF. The Program consists of:

(a) AML/CTF Program Part A; and

(b) AML/CTF Program Part B (Customer Due Diligence Procedures) including the Transaction Risk

Assessment (**TRA**) process.

Part A of the Program sets out the key controls used to identify, assess, mitigate and manage NAIF's assessed ML/TF Risks.

Part A of the Program must be approved and overseen by the NAIF Board. Amendments to the Program may be made over time, and each amendment is effective upon approval by the NAIF Board.

Part B of the Program sets out details of NAIF's customer identification procedures. It also includes the TRA process which sets out NAIF's approach to assessing the risks of a transaction. Part B of the Program is set out in a separate document.

To the extent that NAIF appoints Export Finance to conduct any procedures (other than purely administrative procedures) set out in this Program on its behalf, NAIF will require Export Finance to allow any independent review to include a review of those procedures.

NAIF does not have a Permanent Establishment in a foreign country, hence the AML/CTF Program does not deal with considerations related to such operations.

6. DESIGNATED SERVICES

NAIF conducted a review of the designated services specified in the AML/CTF Act and determined that its loan and guarantee products are designated services under the AML/CTF Act.

NAIF provides, or intends to provide, the following designated services as defined in Table 1 in subsection 6(2) (items 6 & 7 and 48 & 49) of the AML/CTF Act (as amended by the Declaration):

(a) making a loan, where the loan is made in the course of carrying on a loans business or in the capacity of lender for a loan, allowing a borrower to conduct a transaction in relation to that loan; and

(b) guaranteeing a loan, where the guarantee is given in the course of carrying on a business of guaranteeing loans, or in the capacity of guarantor of a loan, making a payment to the lender, where the guarantee was given in the course of carrying on a business of guaranteeing loans.

7. SIZE, NATURE & COMPLEXITY

NAIF is established under the provisions of the *Northern Australian Infrastructure Facility Act 2016* (**NAIF Act**),and is a corporate Commonwealth entity under the *Public Governance, Performance and Accountability Act 2013* (**PGPA Act**).

The PGPA Act sets out the requirements for NAIF in relation to corporate governance, reporting and accountability which are in addition to those in the NAIF Act.

NAIF's financing of infrastructure projects has been assessed as a relatively low ML/TF risk business with funding generally provided to corporates subject to extensive AML/CTF, credit, and reputational due diligence with repayments of the lending facilities generally received from Australian ADI accounts.

The responsible Minister is responsible for the appointment of the Board Members and issuing the NAIF Investment Mandate (currently the *Northern Australia Infrastructure Investment Mandate Direction 2016*) (**Investment Mandate**), as well as having accountability to the Australian Parliament.

The NAIF Board is responsible for deciding, within the scope of the Investment Mandate, the strategies and policies to be followed by NAIF and to ensure the proper, efficient and effective performance of NAIF's functions.

The Chief Executive Officer (**CEO**) of NAIF, is responsible for the day-to-day administration of NAIF, subject to (and in accordance with policies determined by) the NAIF Board.

The CEO is supported by a dedicated team of NAIF Staff and NAIF has entered into a Service Level Agreement (**SLA**) with Export Finance for the provision of additional support services.

The Queensland, Northern Territory and Western Australian Governments will work with NAIF through

the on lending of NAIF investments to project proponents.

The involvement of the states and territory will help to maximise the gains from infrastructure investment in northern Australia. The Investment Mandate contains mandatory criteria for NAIF finance and non-mandatory criteria which must be taken into account by the NAIF Board in determining whether to provide NAIF finance.

8. RISK ASSESSMENT

NAIF is required to have in place appropriate risk-based systems and controls to identify, manage and mitigate ML/TF risks, having regard to the nature, size and complexity of its business and the type of ML/TF risks that it might reasonably face.

NAIF has assessed its ML/TF Risk as set out in Appendix A. NAIF's approach is to incorporate the ML/TF risk assessment methodology into ML/TF risk assessments for each new transaction through the TRA.

Types of ML/TF Risks at NAIF

NAIF's ML/TF Risk profile is divided into the assessment of two major types of risk:
(a) the regulatory risk profile; and
(b) the enterprise risk profile.

Regulatory Risk Profile

NAIF assesses its regulatory risk of breaching the AML/CTF Act and associated regulations or rules. NAIF has committed appropriate resources to identify relevant regulatory risk requirements and has taken appropriate measures to achieve AML/CTF compliance. NAIF undertakes all practical steps to promote an effective set of internal controls embodied in NAIF's TRA process and other procedures to prevent potential breaches from occurring.

Enterprise Risk Profile

Any ML/TF Risks faced by NAIF in the provision of its products and services are mitigated by extensive due diligence processes which focus on identifying and understanding the detail of the transaction and any inherent risks. Diligent application of these processes minimises the risk of NAIF becoming unwittingly involved in or supporting ML/TF.

NAIF's ML/TF Risk assessment analyses the enterprise ML/TF Risk profile in terms of the following elements:

(a) The external and internal environment including:
  (i) the vulnerability to predicate crimes
  (ii) the vulnerability to being used for ML
  (iii) the vulnerability to being used for TF
  (iv) the vulnerability to being used to breach targeted financial sanctions.
(b) nature of the customers including:
  (i) the beneficial ownership of a customer
  (ii) whether the customer or any beneficial owner of the customer is a PEP
  (iii) a customer's source of funds and wealth
  (iv) the control structure of non-individual customers
  (v) the industries and jurisdiction of the customers
(c) services or products offered
(d) mode of product or service delivery (direct or through intermediaries)

NAIF's approach to managing ML/TF Risk at a transaction level incorporates its ML/TF Risk assessment, as well as additional reputational risk factors as set out in the TRA process.

Customers

NAIF is, or intends to be, involved in the provision of one or more loans or guarantees. Pursuant to the Declaration, the customer of:

(a) any loan made by NAIF pursuant to a Master Facility Agreement (as contemplated in the Declaration) is the relevant project proponent

(b) any guarantee made by NAIF under and in accordance with the *Northern Australian Infrastructure Facility Act 2016* (Cth) and the NAIF Investment Mandate is the relevant lender in respect of the loan being guaranteed and the relevant project proponent

NAIF customers are mainly companies and government bodies with some exposure to trusts and partnerships. NAIF does not provide any designated services to individuals.

Ownership of these entities can be in the hands of PEPs.

NAIF obtains a detailed understanding of potential customers through the customer identification procedures as part of its transactional due diligence.

The procedures require information to be collected about customers and then independently verified by a company search in the relevant jurisdiction in which the customer is registered or through several other mechanisms including through a reputable independent agency.

Jurisdiction

The AML/CTF Act provides that AML/CTF Regulations may prohibit or regulate the entry into transactions with residents of prescribed foreign countries. NAIF does not expect to enter into transactions with any resident of any prescribed foreign country. NAIF's risk assessment incorporates the following indicators of ML/TF risk sourced from publicly available reports, indices and information:

1. sanctions, embargoes or similar measures issued or taken by entities such as the United Nations or Australian autonomous sanctions
2. the United States of America International Narcotics Control Strategy Report (INCSR);
3. the Financial Secrecy Index
4. Transparency International Corruption Perception Index
5. FATF Membership
6. FinCen advisory on Jurisdictions Subject to Enhanced Due Diligence/Countermeasures.

In addition, when completing a TRA, Staff also assess jurisdictional risk by considering if the country in question is considered to be an attractive place for tax evasion.

NAIF's mandate limits it to providing support for infrastructure projects in Northern Australia. It is anticipated that each project proponent will be an entity established in Australia.

However, in many instances the beneficial owners of that entity may be resident in another jurisdiction. As part of the TRA, NAIF will assess the ML/TF risk of project proponents, this will include assessing the jurisdictional risk of their beneficial owners.

Services/Products Offered

NAIF's services/products have been assessed for the likelihood that they could be used to facilitate ML/TF as set out in Appendix A.

Any proposed new products or services or proposed changes to existing products or services are subject to legal due diligence, which includes an assessment of the extent to which they give rise to regulatory risks, including the risk of contributing to ML/TF.

Mode of Delivery (Channel)

NAIF offers its services/products to customers directly after finance documents have been signed by all relevant parties and any conditions precedents thereunder have been met.

Generally, NAIF develops a detailed knowledge of its customers through direct contact, sometimes including site visits. NAIF has assessed the impact of the mode of delivery of its services on the likelihood that such services could be used to facilitate ML/TF and this assessment is at Appendix A.

Business Operations

NAIF's business operations have been assessed for the likelihood that they could be used to facilitate ML/TF as set out in Appendix A.

9. RISK MANAGEMENT AND MITIGATION

The roles and responsibilities of the NAIF Board, the NAIF Executive and NAIF Staff are established by this document and form a sound basis for promoting compliance with the AML/CTF Act within all relevant areas of NAIF.

Corporate Governance

NAIF has obtained Board approval of the policies outlined in this document, in accordance with the principles of good corporate governance.

The detailed KYC identification procedures set out in Part B of the Program are approved by CEO in consultation with the AML/CTF Compliance Officer.

Management of Breach

The way NAIF investigates incidents and breaches of this Program depends on whether the incident or breach involves an internal or external party.

Where an incident or breach involves an external party, NAIF investigates and escalates the incident or breach in accordance with the Public Interest Disclosure Policy, and where that is not possible, the Incident Reporting Policy. Where persons involved in an incident or breach are confined to one or more internal parties, i.e. a Staff member, NAIF will investigate the incident or breach using the Public Interest Disclosure Policy.

Depending on the outcome of the investigation, NAIF may be required to submit a suspicious matter report (**SMR**) – see section 18 below.

NAIF may terminate the employment of any Staff member who disregards the importance of the principles set out in this document. As noted above, individual Staff members may be subject to prosecution and legal action by a third party or AUSTRAC if found to have been concerned in, or involved with, a contravention by NAIF of its obligations under the AML/CTF Act or if found to have contravened any other AML/CTF laws and regulations.

9.1 Regulatory affairs

NAIF is committed to upholding the law and taking steps to build a productive relationship with AUSTRAC. NAIF is transparent in all its dealings with AUSTRAC and will make available all resources necessary to comply. In this regard NAIF is committed to complying with both the letter and spirit of the AML/CTF laws.

10. ROLES, RESPONSIBILITIES AND RESOURCES

10.1 Role of the Board

The NAIF Board approves Part A of the Program and provides ongoing oversight in relation to the Program. The CEO reports to each Board Audit and Risk Committee (**BARC**) and Board meeting on regulatory developments as well as compliance activities which may include AML/CTF.

The Program will be assessed for its ongoing applicability when conducting the periodic review of NAIF's Risk Management Framework. Depending on the outcome of that process, subsequent specific review of the Program by the NAIF Board Audit Committee or Board may be appropriate.

10.2 Role of the Chief Executive Officer

The CEO approves Part A of the Program and recommends its approval to the NAIF BARC and Board. The CEO in consultation with the NAIF AML/CTF Compliance Officer approves Part B of the Program, which contains detailed procedures relating to customer identification.

The CEO provides ongoing oversight in relation to the Program and ensures that the Program is sufficiently resourced. The CEO co-ordinates resourcing projections into NAIF's Corporate Plan. The Corporate Plan is ultimately approved by the NAIF Board.

10.3 Role of the AML/CTF Compliance Officer

NAIF's AML/CTF Compliance Officer is based within NAIF's Legal department. The AML/CTF Compliance Officer has the right to access the Chair of the NAIF BARC regarding matters within the NAIF BARC's Charter. That right is enshrined in the Charter. Matters within the scope of the Charter include monitoring compliance with all relevant legislation such as the AML/CTF Act.

The AML/CTF Compliance Officer will be responsible for:

(a) Registering with AUSTRAC and ensuring that information held by the regulator remains current

(b) reporting to the NAIF BARC and Board on NAIF's continual compliance with its obligations under the AML/CTF Act

(c) contributing to the design, implementation and maintenance of internal AML/CTF compliance manuals, policies, procedures and systems

(d) overseeing the AML/CTF compliance and the Staff training program including arranging induction training for new Staff

(e) maintaining a Training Register in the AML/CTF Compliance File and for quarterly checking of compliance with this process

(f) providing leadership and contributing to a culture of AML/CTF compliance

(g) acting as a contact officer with AUSTRAC

(h) arranging regular and independent reviews of the AML/CTF Program to be conducted

10.4 Role of the Execution Teams

The Execution Teams will be responsible for complying with Part A of the AML/CTF Program and associated procedures when arranging for a loan to a prospective borrower. This includes, but is not limited to:

(a) ensuring all applicable customer identification procedures in Part B of the AML/CTF Program are strictly complied with

(b) complying with the requirements in the Enhanced Customer Due Diligence (ECDD) Program

(c) ensuring unusual matters related to a borrower or any related party are escalated to the AML/CTF Compliance Officer immediately

(d) co-ordination and facilitation of borrower KYC refresh and Annual ECDD

(e) proactively contributing to the culture of AML/CTF Compliance

10.5 Role of Human Resources

NAIF's Human Resources department (**HR**) is responsible for managing all Staff screening for any potential ML/TF risk factors that may impact on suitability for employment and promotion within NAIF.

HR is responsible for managing online compliance training including AML/CTF and keeping track of completion. HR (through certification by all Staff) also verify that new Staff have read the NAIF Code of Conduct and other NAIF policies and procedures and have satisfactorily completed the personal background checking and screening process.

11. AML/CTF AWARENESS TRAINING PROGRAM

NAIF provides induction, annual and ongoing training to enable NAIF Staff to understand NAIF's obligations under the AML/CTF Act.

The awareness training is designed to enable NAIF Staff to understand:

(a) NAIF's obligations under the AML/CTF Act and the AML/CTF Rules
(b) the consequences of non-compliance with any such obligations
(c) the types of ML/ TF Risk NAIF might face
(d) the potential consequences of such risks
(e) those processes and procedures provided for by this Program

Initial induction training is provided to all Staff and must be completed within two months of joining NAIF. The AML/CTF Compliance Officer maintains records of completion of induction training. The training incorporates information on NAIF's risk-based approach to AML/CTF compliance, to the extent that this is relevant to the person's role.

The AML/CTF Compliance Officer provides more tailored training to Staff who have greater involvement with NAIF's provision of designated services. This training provides Staff with an understanding of NAIF's obligations under the AML/CTF Act, including the types of ML/TF risks faced by NAIF, the relevant procedures that have been put in place to control those risks and the consequences of non-compliance.

All Staff are required to complete AML/CTF online compliance training annually and attend other internal training sessions on NAIF's procedures. All NAIF Staff attest annually that they have read the Program and other business related policies and procedures, which are set out in the Staff annual attestation.

Whenever internal procedures are updated, relevant Staff receive tailored training so that they are aware of how to comply with the new procedures. The AML/CTF Compliance Officer maintains records of training about NAIF's AML/CTF procedures.

12. STAFF DUE DILIGENCE PROGRAM

NAIF's Staff due diligence process is detailed in the HR Employment Screening procedure and Contract Management Policy.

Pre-employment probity checking is conducted for all Staff subject to standard employment contracts and all temporary Staff with contracts or tenure of longer than 3 months.

Temporary positions with contracts or tenure of less than 3 months are considered to have lower risk

given the short tenure of employment and limited systems access.

NAIF outsources its pre-employment screening program to a third-party provider. The contract with the provider incorporates a service level agreement that stipulates which screening checks must be undertaken. NAIF undertakes periodic reviews of the provider's processes and periodically undertakes a comparative analysis of the provider's services against market peers.

All pre-employment screening reports are reviewed and approved by HR. If the report contains evidence of matters that could give rise to risks for NAIF, HR escalate these issues to the relevant Executive Director and a decision will be made about whether to employ the individual or not. All pre-employment screening reports are retained in HR files.

NAIF has undertaken the following employee role risk assessment to determine which roles are deemed a higher risk of committing a money laundering or terrorism financing offence in the provision of a designated service:

Employee Role	How is role related to the provision of a designated service	Summary of inherent ML/TF risks in the role	Risk rating	Frequency of ongoing screening	Frequency of role-based training
Executive Team	Submit Investment Decision Paper to Board for approval	Product/service offered Jurisdictional considerations	LOW	Five years	Induction & Annual
Execution team members	Collate and verify KYC and E/CDD information	Customer identification	LOW	Five years	Induction & Annual
Portfolio Management	Transaction monitoring	Business operations	LOW	Five years	Induction & Annual
AML/CTF Compliance Officer	Review and approve KYC and E/CDD information	Regulatory	LOW	Five years	Induction & Annual
Risk and Compliance Manager	Approve transaction compliance with relevant legislative requirements	Regulatory	LOW	Five years	Induction & Annual
Chief Financial Officer	Approve funds transfer	Business operations	LOW	Five years	Induction & Annual

NAIF re-screens Staff every five years, when they take on greater responsibility, have more direct client contact or generally move into positions where there is greater risk of facilitating a ML/TF breach. NAIF conducts ongoing screening of those employees in higher risk roles in the following circumstances:

a) every 3 years;

b) when an employee moves into or is promoted to a higher risk role;

c) if an employee in a higher risk role goes on long service leave of greater than 3 months (excluding maternity leave);

d) at the discretion of the AML/CTF Compliance Officer when it is deemed necessary.

As referred to in section 3, NAIF Staff may face disciplinary action if they fail to follow NAIF's AML/CTF procedures. NAIF may terminate the relevant contract or appointment terms of any director, officer or Staff member who is found to have, without reasonable excuse, failed to comply with any of NAIF's AML/CTF related systems, controls or procedures established in accordance with Part A or Part B of this AML/CTF Program.

13. ONGOING CUSTOMER DUE DILIGENCE (OCDD)

NAIF will monitor its customers, business partners and transactions on an ongoing basis to assist the identification, mitigation and management of ML/TF risk. This includes:

(a) monitoring transactions for complex, large and unusual transactions (see section 14);

(b) undertaking enhanced customer due diligence (see section 15); and

(c) undertaking periodic refresh of customer identity information (see section 16).

14. TRANSACTION MONITORING

NAIF undertakes transaction monitoring throughout the life cycle of every transaction:

(a) for loans, NAIF monitors repayments and the credit risk associated with the transaction. Any variations to the expected repayment schedule are noted and the reasons for such variation are investigated and assessed.

(b) for guarantees, NAIF monitors the transaction during the period in which NAIF is “on risk” and the guarantee may be called.

Those products offered by NAIF, which constitute designated services, are relatively illiquid in nature, and have a defined commencement and end date.

The purpose of this transaction monitoring program is to formalise NAIF’s approach to determine whether a customer interaction or transaction is deemed complex, demonstrates unusually large transactions and unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

The TRA process, which incorporates Part B of the Program, also identifies triggers that could indicate unusual activity. These triggers are referred to as ‘red flags’ and can occur at a transaction or customer interaction level. We have identified the following red flags relevant to our business:

(c) Customers who appear overly concerned about the transaction being reported to the authorities;

(d) Unusual or complex transactions with no apparent economic rationale;

(e) Customers who frequently make changes to their address or authorised signatory;

(f) Customers who do not seem to understand the product or service they are requesting or who appear vague about the identity of the beneficiary and their relationship to them;

(g) Customers who exhibit a low level of cooperation when providing all the customer identity information required by Part B customer due diligence standards; and

(h) Early or rapid repayment of the lending facility.

(i) Source of funds (the funds utilised to pay down the lending facility) originate offshore or the borrower seeks to change the source of the repayment.

(j) Any other unusual behaviour by a customer, based on the normal or expected behaviour of a customer using a product or service.

With reference to the red flags for our business, all employees (both NAIF and Export Finance) are required to consider whether a customer interaction or transaction is unusual and, if so, to report it to the AML/CTF Compliance Officer in the first instance.

When an employee escalates an identified red flag, no employee of NAIF or Export Finance must engage in contact with the borrower or a representative of the borrower until clearance is provided by the AML/CTF Compliance Officer.

It is a criminal penalty to inform anyone other than AUSTRAC that a suspicious matter reporting obligation has arisen or that a suspicious matter report has been provided to AUSTRAC. This penalty can carry severe fines and/or 2 years imprisonment.

NAIF and Export Finance employees are made aware of the red flags relevant to our business as part of their AML/CTF Risk Awareness training. The AML/CTF Compliance Officer will review the red flags every 12 months to see if new flags should be added.

Employees must report any red flags identified to the AML/CTF Compliance Officer immediately.

Where a transaction is identified against a red flag or the set of defined unusual characteristics, the AML Compliance Officer may:

(a) Investigate all the recent transaction history of the customer to identify anything that may give rise to a suspicious matter reporting obligation; or

(b) Seek further information from the customer; or

(c) Apply enhanced CDD; and/or

(d) Upon forming a suspicion in accordance with Section 41 of the AML/CTF Act, lodge a suspicious matter report with AUSTRAC.

15. ENHANCED CUSTOMER DUE DILIGENCE (ECDD)

The TRA process requires ECDD to be performed for any of the following:

(a) where the ML/TF Risk is assessed as at least high in an individual transaction

(b) where the relevant customer or a beneficial owner of the customer is a PEP or otherwise a PEP assessed as high risk

(c) where a suspicious matter reporting obligation has arisen, as contemplated in section 18, below

(d) where the relevant customer is incorporated in a prescribed foreign country, as contemplated under the heading 'Jurisdiction' in section 8, above

Where ECDD is required to be undertaken for the first time, the following measures are applied over and above the standard level of due diligence applied by NAIF when making an Investment Decision:

(a) obtain further KYC information or beneficial owner information that provides NAIF with an understanding of:

(i) the source of the borrower's funds (where will the borrower source the money to repay the lending facility – will it be from the activities of the project or from another source i.e. a bank account offshore)

(ii) the source of each beneficial owner's wealth (paying close attention to any history of private ventures on government contracts and whether the beneficial owner has a demonstrated history in the industry the customer is involved in)

(b) undertake more detailed analysis to clarify and document the expected nature and level of future transactional behaviour i.e. is there a likelihood that the customer may rapidly repay the loan from another funding source other than from the operation of the project being funded

(c) obtain the CEO's approval to proceed with the relationship

Where ECDD is required to be undertaken at the point of periodic identity refresh, the following measures are applied:

(a) clarify all customer identification and KYC information held on file and update the information where it has changed

(b) verify all customer identification and beneficial owner information that has changed in accordance with the verification requirements outlined in the applicable customer identification procedures in Part B of this AML/CTF Program

(b) obtain further KYC information or beneficial owner information that provides NAIF with an understanding of:

(i) whether the source of the customer's funds continues to remain the same or has changed

(ii) the source of each beneficial owner's wealth and whether it continues to remain the same or has changed

(b) undertake a detailed analysis of the customer's transactional history to corroborate whether the observed transactional behaviour deviated from the expected nature and level of transactional behaviour during the prior 12 months

(c) obtain the CEO's approval to continue the business relationship with the borrower

Where ECDD is required to be undertaken on the positive identification of a PEP or at the point of periodic identity refresh for a borrower linked to a PEP, the following measures are applied:

(a) undertake a more detailed analysis of the customer's KYC information and beneficial owner information including taking reasonable measures to identify/re-confirm:

(i) the source of each beneficial owner's wealth; and

(ii) the source of the customer's funds;

(b) verify or re-verify customer KYC information in accordance with the customer identification procedures in Part B of this AML/CTF Program;

(c) verify or re-verify beneficial owner information in accordance with the beneficial owner identification requirements specified in Part B of this AML/CTF Program;

(d) undertake more detailed analysis and monitoring of the customer's transactions – both past and expected future activity, including, but not limited to:

(i) the purpose, reasons for, or nature of specific transactions;

(ii) the expected nature and level of transaction behaviour, including future transactions;

(e) seek the CEO's approval for:

(i) beginning/continuing a business relationship with the borrower; and

(ii) whether a designated service should commence/continue to be provided to the borrower;

The TRA process incorporates NAIF's ECDD procedures using its risk assessment methodology.

This methodology is adopted and applied to each transaction in accordance with the TRA process.

The ECDD processes we apply involve seeking enhanced KYC collection and verification additional information about the customer and are set out in Part B. Any enhanced due diligence undertaken requires review and sign off by the AML Compliance Officer (or their delegate). Depending on the outcome, the AML Compliance Officer (or delegate) will:

(a) Approve the customer;

(b) Reject the customer; or

(c) Advise of specific requirements for taking on the customer relationship (e.g. specific ongoing monitoring steps).

The AML Compliance Officer will also decide whether additional approval and ML/TF risk acceptance are required from the senior persons responsible for the management of the business.

We will not accept or maintain a relationship with a customer unless our requests for enhanced due diligence information are satisfactorily met by the customer.

16. PERIODIC IDENTITY REFRESH

NAIF has adopted a risk-based approach to periodically refreshing the identity information of customers, consistent with its approach to initial customer due diligence.

Using this risk-based approach and noting that NAIF provides products where the private market is unable or unwilling to provide financial support to clients, NAIF has designed its systems and controls to clarify and update any KYC or CIP information it becomes aware has changed on a trigger based approach.

The triggers that NAIF monitor for to initiate a refresh of customer or beneficial owner information includes, but is not limited to, the following:

- The Execution team engages in communication with the borrower regarding potential changes to the lending facility;
- The Execution team becomes aware of a change in the borrower's circumstances, including but not limited to, the nature of the borrower's business, the directors, the beneficial owners, the ability to repay the lending facility etc;
- Upon review of the lending facility;
- The borrower seeks an additional lending facility or the directors/beneficial owners enquire about an additional lending facility through another borrowing entity;
- Any other circumstances that may arise regarding the borrower i.e. the borrower, directors or beneficial owners are mentioned in the media.

Where any of the triggers are identified, NAIF confirms with the customer whether the existing information held on file is complete and accurate. Where information has changed, NAIF will document this information as having been changed and ensure that both the old and new information is retained on the file,

Where the customer is low or medium risk, the changes (except for any changes in beneficial ownership) will not be required to be verified. Where there is a change in beneficial ownership, NAIF will verify the new beneficial ownership structure via the reliable and independent documents or electronic-data sources it has deemed acceptable as documented in this AML/CTF Program. In addition, NAIF verifies the identity of each new beneficial owner according to the CIP in Part B of this AML/CTF Program via the reliable and independent documents or electronic-data sources it has deemed acceptable as documented in this AML/CTF Program.

For high risk borrowers, NAIF verifies any changes to the KYC or CIP originally collected and verified from either the original CIP or the previous KYC refresh on an annual basis over and above the annual ECDD undertaken according to this AML/CTF Program.

17. DOCUMENT RETENTION

Subject to any requirements in NAIF's Records and Information Management Policy requiring records to be held for a longer time, NAIF will apply the following document retention requirements to any documents relating to its Program and transactions involving products subject to that Program:

NAIF record	Minimum length of time document must be held prior to disposal
Records relating to the provision of a designated service to a customer	7 years from the date of making the record
Records of identification procedures	7 years after ceasing to provide a designated service to the customer
AML/CTF Program – Parts A & B	7 years after the Program ceases to be in force

18. REPORTING

Suspicious Matter Reporting (SMR)

NAIF will submit a suspicious matter report, where, in relation to a customer or prospective customer, it has reasonable grounds to suspect:

(a) the customer or prospective customer (including any agent of the customer) is not who they claim to be;

(b) information relating to the provision by NAIF of a designated service may be relevant to the investigation or prosecution of:
- evasion of a taxation law;
- an offence against a law of the Commonwealth, State or Territory;
- enforcement of the *Proceeds of Crime Act 2002*;
- an offence of financing of terrorism (as defined in the AML/CTF Act) or the provision or prospective provision by NAIF of a designated service is preparatory to such an offence; and/or
- an offence of money laundering (as defined in the AML/CTF Act) or the provision or prospective provision by NAIF of a designated service is preparatory to such an offence.

An SMR reporting obligation may arise at the earliest of either a person making an enquiry of NAIF regarding a potential transaction involving a designated service or NAIF proposing to provide a designated service to a potential customer.

NAIF has an obligation to report the suspicious matter within 24 hours of forming a suspicion in relation to TF activity or, otherwise, within 3 days of forming the relevant suspicion.

The AML/CTF Compliance Officer or appropriate authorised delegate is responsible for forming a suspicion and submitting an SMR to AUSTRAC in accordance with Section 41 of the AML/CTF Act.

If NAIF or Export Finance staff identify any unusual activity or come across any discrepancies in information provided, they should discuss the matter with their supervisor and if there are reasonable grounds that the circumstances are considered unusual or the reasons for the discrepancies remain unclear, Staff should then immediately report the matter to the AML/CTF Compliance Officer as an unusual activity report.

An SMR obligation arises when the incident has been investigated and the AML/CTF Compliance Officer has determined that a suspicious matter has arisen. NAIF recognises that the SMR reporting obligation is an ongoing one. It continues to apply should NAIF form the relevant suspicion at any time prior to or after it starts providing the designated service to the obligor, or the obligor requests or enquires about the designated service.

During the life of a transaction, ongoing reviews are undertaken. Such reviews are conducted on a risk-based trigger approach (except high risk rated customers), or more often should circumstances warrant. Staff have received training on how to escalate any unusual circumstances to allow NAIF to report a SMR if required to do so.

Threshold Transaction Reporting

NAIF must submit a threshold transaction report (**TTR**) to AUSTRAC if its provision of a designated service involves the transfer of physical currency or e-currency (as defined in the AML/CTF Act) of $10,000 or more (or equivalent). NAIF does not have any obligation to a submit a TTR because the terms on which it provides designated services require all payments to be made by transfer between relevant bank accounts and NAIF does not accept or provide cash payments.

International Funds Transfer Instruction Reporting

NAIF does not have an obligation to submit International Funds Transfer Instructions (**IFTIs**) reports to AUSTRAC because NAIF does not provide facilities for clients to conduct international funds transfers. Any international transfers are made by the respective banks.

Changes to enrolment details reporting

NAIF identifies its obligation to report changes in enrolment details with AUSTRAC within 14 business days pursuant to Section 51F of the AML/CTF Act and Chapter 64 of the AML/CTF Rules.

The way NAIF ensures compliance with this obligation is through carrying out the following procedure:

a) The Board Secretary or Risk and Compliance Manager will inform the AML/CTF Compliance Officer when any information about NAIF or its activities changes i.e. balance sheet size (above a threshold), registered address, company name, etc;

b) Where a change is identified, the AML/CTF Compliance Officer will confirm that the applicable change is required to be reported by cross-referencing the list of items in Chapter 64 of the AML/CTF Rules;

c) Where the change is required to be reported, the AML/CTF Compliance Officer will log-in to AUSTRAC online, confirm the existing information held by AUSTRAC is out of date, and amend the details.

19. AUSTRAC FEEDBACK AND GUIDANCE

AUSTRAC is Australia's AML/CTF regulator overseeing compliance with the AML/CTF Act. AUSTRAC may provide reporting entities, such as NAIF, with feedback in respect of their performance on the management of ML/TF risk. AUSTRAC may also provide guidance, either directly to NAIF or an industry specific report or communication. NAIF considers all AUSTRAC guidance and considers the applicability to NAIF's business.

AUSTRAC also has the power to compel Reporting Entities to produce certain information. The receipt of any notice, direction or recommendation from AUSTRAC will immediately be referred to the AML/CTF Compliance Officer and the Risk and Compliance Manager.

NAIF's procedure to respond to any feedback or guidance (where applicable) provided by AUSTRAC is to table the correspondence together with the NAIF recommended response at the NAIF BARC meeting immediately following receipt of such feedback and guidance.

20. REVIEW

Part A of the Program is subject to regular, independent review by a competent reviewer. The review shall assess:

(a) the effectiveness of Part A of this Program having regard to NAIF's ML/TF risk;
(b) whether Part A of this Program complies with the AML/CTF Rules;
(c) whether Part A of this Program has been effectively implemented; and
(d) whether NAIF has complied with Part A of this Program.

NAIF also arranges for a review by the independent reviewer, of Part B of the Program (Customer Due Diligence Procedures) at or about the same time as the Part A review; including customer and beneficial owner due diligence, and the TRA.

In addition, the AML/CTF Compliance Officer provides ongoing updates to the NAIF Board Audit and Risk Committee and on the status of the Program and any issues.

21. MONITORING COMPLIANCE

The AML/CTF Compliance Officer will monitor compliance with this Program. A Section 47 Annual Compliance report must be completed and submitted to AUSTRAC on an annual basis for the reporting period of 12 months beginning on 1 January and ending on 31 December of the prior year.

The lodgement period in which NAIF will submit its Section 47 Annual Compliance report is specified to be the period of 3 months beginning at the end of each successive reporting period i.e. 3 months from 31 December.

NAIF will undertake the following steps in compiling the Section 47 Annual Compliance report before submitting the completed questionnaire to AUSTRAC:

a) The AML/CTF Compliance Officer confirms all the responses to the questionnaire in the report with relevant stakeholders and the Risk and Compliance Manager with a clear focus on accuracy of the responses provided;

b) The AML/CTF Compliance Officer submits a draft of the questionnaire to the NAIF CEO for consideration and approval;

c) Once approved, the AML/CTF Compliance Officer will submit the Section 47 Annual Compliance Report to AUSTRAC via the AUSTRAC portal in the stipulated format and timeframe.

All NAIF Staff are required to complete an annual compliance attestation, which includes confirmation of compliance with NAIF's policies, including the AML/CTF Program and completion of relevant compliance training on AML/CTF. All compliance issues in respect of the application of the Program must be communicated to the AML/CTF Compliance Officer. In responding to such issues, relevant factors to be considered will be:

(a) what records have been maintained and enquiries made in relation to the issue;
(b) whether compliance measures need to be reviewed; and
(c) whether the breach register has been completed.

Compliance breaches will be escalated in accordance with NAIF's Incident Reporting Policy.

Appendix A - Enterprise ML/TF Risk Assessment

Australian Government

Northern Australia Infrastructure Facility

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING (AML/CTF) PROGRAM

PART B including Transaction Risk Assessment (TRA) Process

May 2020

www.naif.gov.au

Contents

1. Purpose 3
2. Scope 3
3. Process 3
Attachment 1 – Collection and Verification of KYC Information 8
KYC Collection and Verification Requirements 9
Attachment 2 – NAIF Transaction Risk Assessment (TRA) Form 16

Document Review and Approval

VERSION	AUTHOR/OWNER	REVISION	APPROVAL	DATE OF APPROVAL	NEXT REVIEW DATE
1.0	General Counsel	Original	Board	January 2018	January 2019
2.0	General Counsel	Annual review	Board	February 2019	February 2020
3.0	Risk and Compliance Manager	Independent review	Board	7 May 2020 TBC	February 2021

NAIF Transaction Risk Assessment (TRA) Process

1. Purpose

The primary purpose of this Part B AML/CTF Program is to document the applicable customer identification procedures to be applied by NAIF before it provides a designated service to the relevant customer.

NAIF assesses certain risks, including the ML/TF Risk, of its provision of a designated service to a customer in accordance with the Transaction Risk Assessment (**TRA**) process set out in this document.

2. Scope

The applicable customer identification procedures and TRA set out in this document must be carried out before the entry by NAIF into documentation relating to its provision of any designated service, including making any loan or guaranteeing a loan.

For the avoidance of doubt, a TRA is not required for NAIF to enter into a Master Facility Agreement (**MFA**) with the Commonwealth, States or Northern Territory because a MFA does not give effect to the provision by NAIF of any designated service.

Capitalised terms used in this Part B AML/CTF Program have the meaning given in Part A of NAIF's AML/CTF Program, unless otherwise defined or the context requires otherwise.

3. Process

Execution team members should consider the potential risks, including ML/TF Risk and reputational risk to NAIF, the Commonwealth and the relevant State or Territory, arising from the transaction as a whole, not simply the risks associated with providing a loan or financing mechanism to a particular project proponent.

A TRA, incorporating the applicable customer identification procedure in respect of each prospective customer, must be completed for each new transaction prior to NAIF entering into contractual arrangements to give effect to a loan or other financing mechanism, including by way of guaranteeing a loan.

Where a Project is subject to conditional credit approval, an interim TRA must be completed documenting known risks at the time of conditional credit approval and then the TRA must be updated and finalised prior to entering into contractual arrangements to give effect to a loan or other financing mechanism.

3.1 Identify Parties Relevant to the Transaction

In addition to the applicable customer identification required under section 3.3 below, the responsible Execution team member must identify all relevant parties to the transaction from a risk perspective (including in respect of reputational risk and ML/TF Risk) such as:

- the project proponent;
- owners and ultimate beneficial owners of the project proponent;
- joint venture partners in any special purpose vehicle (SPV) used to develop the project;
- subcontractors to the project;
- suppliers to the project;
- agents of the project;
- off-takers of any end product of the project; and
- directors, CEO and senior executive management of the above parties.

3.2 Undertake Due Diligence Searches

The responsible Execution team member must undertake the following searches:

- Company searches of the customer (project proponent) and its owners;
- Dow Jones searches of all relevant parties; and
- Google searches of all relevant parties.

Note: for infrastructure projects involving a very large number of subcontractors, consultants, agents or suppliers, the Execution team member must make a risk-based judgement on the level of due diligence searches to be conducted and document this decision in the TRA. Search results must be attached to the TRA.

3.3 Customer Identity Collection and Verification

Execution team members must undertake the applicable customer identification procedure in respect of each customer (within the meaning of the Declaration) as set out in Attachment 1. Depending on the nature of the customer, different identification and verification requirements apply.

3.4 Customer Risk Assessment

NAIF considers the following factors in determining a ML/TF Risk rating for a customer:

i) the type of customer (including any PEPs associated with the customer and industry of the customer);
ii) the customer's sources of funds and wealth;
iii) the control structure of the customer;
iv) the nature and purpose of the customer's business relationship with NAIF;
v) the jurisdiction in which the customer is established and in which its beneficial owners are resident;
vi) the designated services provided or proposed to be provided to the customer; and
vii) delivery channels of those designated services to the customer.

3.4.1 Customer

NAIF will undertake a detailed analysis of each customer, its owners and beneficial owners to determine the ML/TF risk level associated with the customer in each TRA.

NAIF does not generally accept a disclosure certificate as a verification source. The decision to rely on a disclosure certificate as a verification source for the purposes of the applicable customer identification procedure must be escalated to the AML/CTF Compliance Officer for approval.

Politically Exposed Persons (PEPs)

As part of the assessment of the customer, Execution team members should also identify any PEP associated with the customer, including any beneficial owner who is a PEP.

PEPs are categorised into three distinct groups:

- Domestic PEPs;
- Foreign PEPs;
- International Organisation (i.e. UN, FIFA, Bank for International Settlements, World Bank etc) PEPs

A PEP is a person who might be expected to exert political influence in their society. Typically, this occurs when a person holds or has been entrusted with a prominent public function in a government body or an international organisation. Examples of PEPs include:

- Government Members (Federal, State & Local)
- Members of the Legislative Body (Federal, State & Local)
- Heads of State
- Senior civil servants
- Senior embassy and consular staff
- Senior members of the armed forces
- Senior members of the police force
- Senior members of the judiciary
- Senior members of the secret services
- Senior executives of state-owned corporations or enterprises
- Governors of central banks
- Senior Political Party Officials
- Senior Officials of Political Pressure Groups
- National Non-Government Organisation (NGO) Officials
- Religious Leaders
- Senior members of international organisations.

Immediate family members and close associates of any such person are also PEPs. For that purpose:

- a close associate of a person means any individual who is known (having regard to information that is public or readily available) to have:
  - joint beneficial ownership of a legal entity or legal arrangement with that person; or
  - sole beneficial ownership of a legal entity or legal arrangement that is known to exist for the benefit of that person; and
- an immediate family member includes a parent, a spouse, a de facto partner, a child or a child's spouse or de facto

partner.

The involvement of PEPs in a transaction may be a risk factor in the transaction, since PEPs are in a position to engage in corrupt behaviour or to facilitate illicit transactions. This is not to suggest that all PEPs are corrupt but identifies PEPs as a potential risk factor in the transaction.

Once a person no longer holds a prominent public position, or is no longer connected to someone holding a prominent public position, NAIF will continue to apply a risk-based approach to determining whether they should be considered a potential risk factor in the transaction. Higher risk PEPs are more likely to continue to wield political influence even after they have ceased to hold a prominent public position.

For all PEPs (within the meaning of AML/CTF Rules) NAIF will:

- take reasonable measures to establish the PEP's source of wealth and source of funds;
- identify the PEP in accordance with the 'individual identification' requirements set out in Appendix 1;
- obtain CEO approval before establishing or continuing a business relationship with the individual and before the provision, or continued provision, of a designated service to the customer; and
- apply the enhanced customer due diligence procedures set out in Part A of the AML/CTF Program. If the PEP is closely linked to NAIF's customer (i.e. part of its ownership and control structure) then it is reasonable for NAIF to require the customer to provide this information.

If the PEP is not part of its ownership and control structure, then it is reasonable to undertake public source information searches. Execution team members should exercise judgement in determining how to obtain information relating to the PEP's source of wealth and source of funds. When in doubt please consult the AML/CTF Compliance Officer.

Industry

Execution team members should identify the primary industry of the customer to which NAIF's support relates. Where a customer is involved in multiple industries, the industry that is the subject of NAIF's proposed support should be selected.

The following industries are categorised as very high risk:

- Military;
- Gambling;
- Live animal exports;
- Space & aeronautical;
- Dual-use military equipment; and
- Manufacturing, trading or wholesaling jewellery and precious gems.

The following industries are categorised as moderately high risk:

- Construction;
- Real estate;
- Mining and extractive industries;
- Refining or manufacturing of non-renewable energy products;
- Property development;
- Non-retail banking; and
- Cargo ship or plane chartering.

These risk categorisations are based on knowledge and experience, with reference to potential sectors NAIF may finance, and following consultation between NAIF, Export Finance and Grant Thornton. Generally other industries will be classified as low risk, although Execution team members should exercise their own judgment in making this assessment.

3.4.2 Jurisdiction

NAIF's Investment Mandate limits it to providing support for infrastructure projects based (in whole or in part) in Northern Australia. Where infrastructure projects chosen for NAIF finance are based partly outside of Northern Australia, it is envisaged that these projects will be based in another part of Australia. The ML/TF jurisdictional risk of the infrastructure projects that NAIF will finance is therefore considered low.

However, the jurisdiction of customers or beneficial owners is to be considered as follows. It is anticipated that each project proponent will be an entity established in Australia. In many instances, the beneficial owners of that entity may be resident in another jurisdiction. The TRA risk rating score should consider the ML/TF Risk associated with each such jurisdiction, with regard to:

- sanctions, embargoes or similar measures issued or taken by entities such as the United Nations or Australian autonomous sanctions;
- the United States of America International Narcotics Control Strategy Report (INCSR);
- the Financial Secrecy Index;
- Transparency International Corruption Perception Index;

- FATF Membership; and
- FinCen advisory on Jurisdictions Subject to Enhanced Due Diligence/Countermeasures; and
- any other relevant circumstances.

Products and Services

NAIF is, or intends to be, involved in the provision of one or more loans or guarantees.

On the basis of the risk assessment annexed to Part A of the AML/CTF Program, NAIF has assessed the inherent risk:

- of providing a loan as low; and
- of providing a guarantee as low.

The TRA risk rating score is to be adjusted accordingly.

Delivery Channel

Generally, NAIF is expected to use a direct delivery channel. On the basis of the risk assessment annexed to Part A of the AML/CTF Program, NAIF has assessed the ML/TF risk of direct delivery channels as being low. Accordingly, this is reflected in the TRA risk rating score.

Indicators of a direct delivery channel are:

- Face to face meetings with a project proponent;
- Direct emails, correspondence and telephone calls from representatives of the project proponent; and
- Site visits to the proposed project site.

An example of an indirect delivery channel would be an online loan application where a person does not have to speak to, or have any face to face contact with, the loan provider. The customer risk analysis and rating must consider the ML/TF Risk associated with any such delivery channel.

3.4.3 Customer Risk Analysis and Rating

The Execution team member should make a qualitative risk assessment for the customer taking into account information obtained about:

- the customer (including the type of customer and its control structure);
- the customer's beneficial owners;
- any PEPs associated with the customer;
- the customer's source of funds and wealth;
- the customer's industry;
- the nature and purpose of NAIF's business relationship or proposed business relationship with the customer;
- jurisdiction of the customer's registered address and thejurisdiction of residence of its beneficial owners;
- the product provided, or proposed to be provided, to the customer; and
- the delivery channels by which NAIF provides, or proposes to provide, the relevant product to the customer.

3.5 Enhanced Customer Due Diligence

3.5.1 KYC Collection and Verification

Execution team members must consider and complete enhanced KYC collection and verification if the risk score is "high" and the transaction involves the provision by NAIF of a designated service (see section 15 of Part A of the AML/CTF Program).

The enhanced KYC collection and verification includes the collection and verification of any further information about the customer not already obtained or verified as required by the applicable customer identification procedure in Part B of this AML/CTF Program. The Execution team must follow the Enhanced Customer Due Diligence Procedure relevant to the specific scenario as outlined in Section 15 of the AML/CTF Rules.

3.6 Risk Analysis and Recommendation

The Execution team member must insert written commentary on the risks of the transaction with an overview of key risks, including ML/TF Risk and any reputational risks, relating to the transaction as a whole, not just the relationship with a particular risk party.

Such risk factors can arise from information obtained through conducting searches or otherwise (for example from press reports.)

Execution team members should analyse the results of the searches and include information about incidents or adverse media reports contained in Dow Jones and Google searches.

Relevant information would be findings or allegations of fraud, corruption, bribery, money-laundering, breaches of sanctions or other matters that suggest the entity does not have appropriate policies and procedures or has poor governance. Only those incidents or financial crimes that have taken place during the last 10 years need to be included.

Following the risk analysis, the Execution team member must make a recommendation on whether the transaction should be approved.

When in doubt please consult the AML/CTF Compliance Officer.

Attachment 1 – Collection and Verification of KYC Information

Note the tables below set out the customer collection and verification requirements for different types of entities.

The term 'beneficial owner' includes both an individual who owns (directly or indirectly) 25% or more of the entity and a person who exercises management control over an entity (being someone who has the capacity to determine decisions about financial and operating policies of the entity, such as the CEO or CFO.)

For beneficial owners, electronic verification using SAI Global (or other appropriate service provider) is the primary verification source.

If unable to verify the identity of a beneficial owner electronically, NAIF will undertake manual verification of the person's identity as follows:

Request certified copies of photographic identification documents (current passport and driver's licence) in order to verify the identity of each beneficial owner. The list of persons who can certify documents is set out below:

- Notary public (authorised in Australia or in a foreign country);
- Employee of the Australian Trade Commission who is:
  - in a country or place outside Australia; and
  - authorised under paragraph 3(d) of the Consular Fees Act 1955; and
  - exercising his or her function in that place
- Employee of the Commonwealth who is:
  - in a country or place outside Australia; and
  - authorised under paragraph 3(c) of the Consular Fees Act 1955; and
  - exercising his or her function in that place
- Registered Legal practitioner (or equivalent in the jurisdiction); and
- Chartered Accountant (or equivalent in the jurisdiction).

Where the documents are provided in a language other than English, it is necessary that English versions are provided by the customer. All documents must be translated in their entirety by a professional person e.g. lawyer or a legal translator.

A translated document must be certified by the translator. The translator must confirm in writing on the translation:

- That it's a 'true and accurate translation of the original document'
- The date of the translation
- The full name and contact details of the translator or a representative of the translation company Any discrepancies in information identified will require

a satisfactory explanation from the customer.

If NAIF is not reasonably satisfied that the customer is who they claim to be or the discrepancy has not been satisfactorily explained, the matter must be referred immediately to the AML/CTF Compliance Officer.

NAIF has determined through the following risk assessment (completed in accordance with Parts 4.9 and 4.10 of the AML/CTF Rules) that the documents and electronic-data sources referred to in the customer identification tables are reliable and independent for the purposes of carrying out the customer identification procedures for each customer entity type and for individual beneficial owners/controllers:

Data Source Name	Summary of electronic-data source	a) The accuracy of the data	b) How secure the data is	c) How the data is kept up to date	d) Whether the data has been verified from a reliable and independent source	f) Whether the data is maintained by a government body or pursuant to legislation	g) Whether the electronic data can be additionally authenticated	Conclusion
Australian Electoral Roll	All persons currently registered to vote will appear on the electoral roll.	The data is maintained by the Federal Government.	Data is safeguarded against unauthorised access	Accessed real time. Reliant on information being updated on individuals but individuals need updated info to vote	Data is reliable because to enrol one requires a driver's licence or Australian passport number or have someone who is enrolled to confirm your identity. The data is independent of other sources apart from the State Electoral Rolls	The data is secure and is kept up to date by the AEC. The data is accurate, up to date with updates being made in real time and deployed on a weekly basis.	Potential to however could be out of our ability to authenticate the data	Reliable and independent source
Data Co-Op	Hosted by D&B and provided by the company Greater Data. This data source comprises more than 16 million records aggregated from Greater Data's data partners. The nature of Personal Information collected by Greater Data may include information such as an individual's name, address, business/company name,	Data is continuously cleansed to ensure information is accurate and valid. Greater Data collects information from consumers directly and publicly available sources such as Australia Post, Australian Electoral Commission, Telstra, ASIC,	Data is stored in Australia in secured environments with access restricted to authorised personnel only and in compliance with Australian Privacy Principles	The Data Co-Op database is completely re-built every month with all major contributors refreshing their data sets.	The data source is continually reviewed by D&B to ensure a consistent and quality outcome when verifying individuals in compliance with AML/CTF	This database is run by a private company	Potential to however could be out of our ability to authenticate the data	Reliable and independent source

	role/position, business information, telephone numbers, email address, bank account details, credit history, Australian Business Number, driver's licence number, and photograph.	and ACMA.						
Australian Claims Database	This data source contains information derived from Australian insurance claims and enquiries. The data is accurate, reliable and independent of other sources used.	ACD contains records of approximately 11 million individuals and 700,000 corporate entities.	Data is collected in accordance with the Australia Privacy Policy and is hosted and maintained by D&B. Data is safeguard against unauthorised access.	Refreshed at least monthly	Reliable and independent given there is no other insurance database, and it needs to be reliable because it is illegal to provide false and misleading information to insurance providers.	This database is run by a private company.	Potential to however could be out of our ability to authenticate the data	Reliable and independent source
Australian Tenancy File	This file contains the details of Australian tenants living in rental properties. Data includes tenant blacklist screening, rental history, bankruptcy information, court judgments and court writs.	The real estate industry and major database operators have a stated commitment to fairness and accuracy in the operation of databases. However,	The real estate industry and major database operators have a stated commitment to compliance with their obligations under the Privacy Act.	The data is queried in real time and updates are made daily or ad-hoc, as required.	All applications undertake a 100-point ID assessment to verify their identity and comprises of more than 2 million records.	These databases are run by private companies, not by the Government.	Potential to however could be out of our ability to authenticate the data	Reliable and independent source

		databases may sometimes contain information which can be out of date. (e.g. addresses)						
DVS: Drivers Licence (all states), Australian Passport, Citizenship Certificate, Medicare Card, Birth Certificate	DVS is a secure online system that enables organisations to confirm that information presented on identity documents matches that held by the document issuing agency.	These verifications are conducted in real time to inform decisions that rely upon the confirmation of a person's identity.	DVS is not a database therefore it does not store personal information. Any requests to verify a document via DVS are encrypted and sent via a secure communications pathway.	DVS updates in real time	DVS allows organisations to take information taken from a person's identity document (with their consent) and compare this to a corresponding record of the document issuing agency. Therefore, this is a reliable and independent service. Identity documents that can be verified by the DVS include, but are not limited to, passports and visas, birth certificates, driver licences, and Medicare cards	This database is run by a private company and not by the Government.	Yes, information can be additionally authenticated by requesting certified copies of original documents.	Reliable and independent source (http://www.austrac.gov.au/document-verification-service-and-individual-customer-and-beneficial-owner-identification)

NAIF has determined that when performing the Transaction Risk Assessment process on a prospective borrower, if any of the risk factors are identified as high risk, NAIF will collect/clarify the following additional information about the customer:

- Seek to understand the beneficial owner's source of wealth and source of funds;
- Determine whether the borrower and beneficial owners have a demonstrated history in their industry;
- Document the reasons why the borrower could not obtain lending facilities from the commercial banks;
- Clarify the intended source of funds for the proposed transaction i.e. where will the funds originate from to repay the loan.

Where NAIF has identified that all of the risk factors under the Transaction Risk Assessment are high risk, NAIF will verify the above list of information.

KYC Collection and Verification Requirements

Australian Proprietary Company or Unlisted Public Company Identification and Verification

Identification – collect from the company:	**Verification – verify from reliable and independent documentation or electronic data**
Full name of the company	Required minimum due diligence: obtain ASIC search
Full address of the company's registered office	**Not required** for minimum due diligence but additional verification from ASIC search
Full address of the company's principal place of business (if different)	**Not required** for minimum due diligence but additional verification from ASIC search
ACN	Required minimum due diligence: ACN **-** shown in ASIC search
Whether it is registered as a proprietary or public company	Required minimum due diligence: whether proprietary or public company - shown in ASIC search
The name of each director	**Not required** for minimum due diligence but additional verification from ASIC search
The following information for each beneficial owner: • Name • Address • Date of birth • Driver's licence number and expiry date • Passport number and expiry date	Electronic search of each beneficial owner Or Certified copy of current driver's licence and passport with English translations to verify the individual's: • Name; and • Address ***or*** date of birth

Foreign Proprietary Company registered in Australia - Identification and Verification

Identification – collect from the company:	**Verification – verify from reliable and independent documentation or electronic data**
Full name of the company	Minimum due diligence – shown in ASIC search
Full address of the company's registered office in Australia	**Not required** for minimum due diligence but additional verification from ASIC search
Full address of the company's principal place of business in Australia (if any) or full name and address of the company's local agent in Australia (if any)	**Not required** for minimum due diligence but additional verification from ASIC search
The country in which the company was formed, incorporated or registered	**Not required** for minimum due diligence
Whether it is registered by the relevant foreign registration body, and if so, whether it is registered as a proprietary or public company in its jurisdiction of foreign registration	Minimum due diligence - whether it is registered as a proprietary or public company shown (in order of preference): • foreign jurisdiction company search; or • verification by a reputable, independent agency e.g. Dun & Bradstreet search; or • verification by a reputable local law firm or reputable, international accountancy practice with a local office; or • verification by a reputable local banker
ARBN	Minimum due diligence - ARBN **-** shown in ASIC search
The name of each director	**Not required** for minimum due diligence but additional verification from ASIC search
The following information from each beneficial owner: • Name • Address • Date of birth • Driver's licence number and expiry date • Passport number and expiry date (English translations must be provided for foreign documents)	Electronic search Or Certified copy of current driver's licence and passport with English translations to verify the individual's: • Name; and • Address ***or*** date of birth

Australian listed public company

(or majority owned subsidiary of an Australian listed public company)

Identification – collect from the company:	**Verification – verify from reliable & independent documentation or electronic data**
Full name of the company	ASIC search or stock exchange search
Full address of the company's registered office in Australia	**Not required**
Full address of the company's principal place of business in Australia (if any)	**Not required**
ACN	**Not required**
That the company is an Australian listed public company or a majority owned subsidiary of an Australian listed public company	ASIC search or stock exchange search

Foreign Proprietary Company not registered in Australia - Identification and Verification

Identification – collect from the company:	**Verification – verify from reliable and independent documentation or electronic data**
Full name of the company	Minimum due diligence (in order of preference): • foreign jurisdiction company search; or • verification by a Dow Jones search; or • verification by a reputable, independent agency e.g. Dun & Bradstreet search; or • verification by a reputable local law firm or reputable, international accountancy practice with a local office; or • verification by a reputable local banker
The country in which the company was formed, incorporated or registered	**Not required** for minimum due diligence but additional verification by Dow Jones search
Whether it is registered by the relevant foreign registration body, and if so, whether it is registered as a proprietary or public or some other type of company in its jurisdiction of foreign registration	Minimum due diligence as shown (in order of preference): • foreign jurisdiction company search; or • verification by a reputable local law firm or reputable, international accountancy practice with a local office.
If it is registered by the relevant foreign registration body, any identification number issued by the relevant foreign registration body	Minimum due diligence as shown (in order of preference): • foreign jurisdiction company search; or • verification by a reputable local law firm or reputable, international accountancy practice with a local office.
If it is registered by the relevant foreign registration body, the full address of the company in its country of formation, incorporation or registration as registered by the relevant foreign registration body	**Not required** for minimum due diligence but additional verification from Dow Jones search
If it is not registered by the relevant foreign registration body, the principal place of business in its country of formation or incorporation	**Not required** for minimum due diligence
The name of each director	**Not required** for minimum due diligence but additional verification from Dow Jones search
The following information from each beneficial owner: • Name • Address • Date of birth • Driver's licence number and expiry date • Passport number and expiry date (English translations must be provided for foreign documents)	Electronic search Or Certified copy of current driver's licence and passport with English translations to verify the individual's: • Name; and • Address ***or*** date of birth

Foreign Public Company not registered in Australia - Identification and Verification

Identification – collect from the company:	**Verification – verify from reliable and independent documentation or electronic data**
Full name of the company	Minimum due diligence (in order of preference): • Foreign stock exchange search; or • foreign jurisdiction company search; or • Dow Jones search
The country in which the company was formed, incorporated or registered	**Not required** for minimum due diligence but additional verification by Dow Jones search
Whether it is registered by the relevant foreign registration body, and if so, whether it is registered as a proprietary or public company in its jurisdiction of foreign registration	Minimum due diligence: Foreign stock exchange search
If it is registered by the relevant foreign registration body, any identification number issued by the relevant foreign registration body	**Not required** for minimum due diligence
If it is registered by the relevant foreign registration body, the full address of the company in its country of formation, incorporation or registration as registered by the relevant foreign registration body	**Not required** for minimum due diligence
If it is not registered by the relevant foreign registration body, the principal place of business in its country of formation or incorporation	**Not required** for minimum due diligence
The name of each director	**Not required** for minimum due diligence
The following information from each beneficial owner: • Name • Address • Date of birth • Driver's licence number and expiry date • Passport number and expiry date (English translations must be provided for foreign documents)	Electronic search Or Certified copy of current driver's licence and passport with English translations to verify the individual's: • Name; and • Address ***or*** date of birth

Trust Identification and Verification

Identification – collect from the trustee:	**Verification – verify from reliable and independent documentation or electronic data**
Full name of the trust	Minimum due diligence (in order of preference): • Trust deed; or • Certified copy of trust deed or certified extract from trust deed
Full name and address of the trustee(s)	Verify names of trustee(s) from (in order of preference): • Trust deed; or • Certified copy of trust deed or certified extract from trust deed. Not required to verify the address of trustee(s)
The country in which the trust was established	**Not required** for minimum due diligence
The type of trust (e.g. registered managed investment scheme or unregistered trust established under a trust deed)	**Not required** for minimum due diligence
If any of the trustees is an individual, the information required to be collected from an individual, in respect of one of those individuals	Minimum due diligence as per the verification procedures for individuals
If any of the trustees is a company, the information required to be collected from a company in respect of one of those companies	Minimum due diligence as per the verification procedures for companies
If the initial contribution to the trust was greater than AUD 10,000, the full name of the settlor of the trust	Minimum due diligence (in order of preference): Trust deed; or Certified copy of trust deed or certified extract from trust deed
Full name and address of each beneficiary or details of the class of beneficiaries if the terms of the trust identify beneficiaries by membership of a class	Minimum due diligence (in order of preference): • Trust deed; or • Certified copy of trust deed or certified extract from trust deed And For each identified beneficiary undertake Electronic searches

Partnership Identification and Verification

Identification – collect from the partnership:	**Verification – verify from reliable and independent documentation or electronic data**
Full name of the partnership	Minimum due diligence (in order of preference): • Partnership agreement; or • Certified copy or certified extract from the partnership agreement
Full registered business name as registered by any State or Territory business name authority	**Not required** for minimum due diligence but additional verification from Dow Jones search
Full name and residential address of each partner (except where the partnership is regulated through current membership of a relevant professional association)	**Not required** for minimum due diligence but additional verification of names from (in order of preference): • Partnership agreement; or • Certified copy or certified extract from the partnership agreement
The country in which the partnership was established	**Not required** for minimum due diligence
In respect of one of the partners, the information that would be required to be collected from an individual (see below)	Minimum due diligence as per the verification procedures for individuals
The following information from each beneficial owner: • Name • Address • Date of birth • Driver's licence number and expiry date • Passport number and expiry date (English translations must be provided for foreign documents)	Electronic search Or Certified copy of current driver's licence and passport with English translations to verify the individual's: • Name; and • Address ***or*** date of birth

Individual Verification

The following minimum collection is required for individuals who are partners in a partnership or trustees of a trust. NAIF does not provide designated services to individuals.

Identification – collect from the individual:	**Verification – verify from reliable and independent documentation or electronic data**
Full name	**Electronic Verification** Electronic search **Manual Verification** (where unable to perform electronic verification): Minimum due diligence: e.g. driver's licence (or certified copy) e.g. passport (or certified copy) e.g. national identity card (or certified copy) If unable to verify from primary photographic identification document, can obtain both: a) primary non-photographic identification document e.g. birth certificate, citizenship certificate (or certified copy); and b) secondary non-photographic identification document being a notice issued by a Commonwealth, State, Territory or local government in the preceding 12 months, e.g. Tax Office notice, rates notice, utility notice (or certified copy).
Residential address **AND** date of birth	Minimum due diligence verify either residential address **OR** date of birth: e.g. driver's licence e.g. passport e.g. national identity card If unable to verify from primary photographic identification document, can obtain both: a) Primary non-photographic identification document e.g. birth certificate, citizenship certificate (or certified copy); and b) Secondary non-photographic identification document being a notice issued by a Commonwealth, State, Territory or local government in the preceding 12 months, e.g. Tax Office notice, rates notice, utility notice (or certified copy).

Government Body Identification and Verification

Identification – collect from the body:	**Verification – verify from reliable and independent documentation or electronic data**
Full name of the body	Minimum due diligence (in order of preference): • company search; or • verification by a Dow Jones search; or • verification by a reputable, independent agency e.g. Dun & Bradstreet search; or • verification by a reputable local law firm or reputable, international accountancy practice with a local office; or • verification by a reputable local banker
Full address of the body's principal place of operations	Minimum due diligence (in order of preference): • company search; or • verification by a Dow Jones search; or • verification by a reputable, independent agency e.g. Dun & Bradstreet search; or • verification by a reputable local law firm or reputable, international accountancy practice with a local office; or • verification by a reputable local banker
Whether the government body is an entity or emanation, or is established under legislation, of the Commonwealth or a State, Territory or foreign country, and if so the name of the State, Territory or foreign country	Minimum due diligence (in order of preference): • company search; or • verification by a Dow Jones search; or • verification by a reputable, independent agency e.g. Dun & Bradstreet search; or • verification by a reputable local law firm or reputable, international accountancy practice with a local office; or • verification by a reputable local banker
If a foreign government body, collect information about the ownership and control of a government body. Collect the following information from each beneficial owner: • Name • Address • Date of birth • Driver's licence number and expiry date • Passport number and expiry date (English translations must be provided for foreign documents)	Make a risk-based determination about whether to verify this information by (in order of preference): • company search; or • verification by a Dow Jones search; or Electronic search of individuals Or Certified copy of current driver's licence and passport with English translations to verify the individual's: • Name; and • Address ***or*** date of birth

Registered Co-operative Identification and Verification

Identification – collect from the partnership:	**Verification – verify from reliable and independent documentation or electronic data**
Full name of the co-operative	Minimum due diligence (in order of preference): • ASIC search or extract from the State, Territory or overseas body responsible for the registration of the co-operative; • Any register maintained by the co-operative; or • Certified copy or certified extract from any register maintained by the co-operative
Full address of the registered office or principal place of operations (if any) of the residential address of the co-operative's secretary or (if there is no such person) the co-operative's president or treasurer	**Not required** for minimum due diligence
Any unique identifying number issued to the co-operative upon its registration by the State, Territory or overseas body responsible for the registration of the co-operative	Minimum due diligence (in order of preference): • ASIC search or extract from the State, Territory or overseas body responsible for the registration of the co-operative; • Any register maintained by the co-operative; or • Certified copy or certified extract from any register maintained by the co-operative
Full name of the chairman, secretary and treasurer or equivalent officer in each case of the co-operative	**Not required** for minimum due diligence
The following information from each beneficial owner: • Name • Address • Date of birth • Driver's licence number and expiry date • Passport number and expiry date (English translations must be provided for foreign documents)	Electronic search Or Certified copy of current driver's licence and passport with English translations to verify the individual's: • Name; and • Address ***or*** date of birth

Incorporated Association Identification and Verification

Identification – collect from the partnership:	**Verification – verify from reliable and independent documentation or electronic data**
Full name of the association	Minimum due diligence (in order of preference): • Partnership agreement; or • Certified copy or certified extract from the partnership agreement
Full address of the registered office or principal place of administration (if any) or the residential address of the association's public officer or if there is no such person) the association's president, secretary or treasurer	**Not required** for minimum due diligence
Any unique identifying number issued to the association upon its incorporation by the State, Territory or overseas body responsible for the incorporation of the association	Minimum due diligence (in order of preference): • ASIC search or extract from the State, Territory or overseas body responsible for the registration of the association; • Constitution or rules of the association; • Certified copy or certified extract of constitution or rules of the association;
Full name of the chairman, secretary and treasurer or equivalent officer in each case of the association	**Not required** for minimum due diligence
The following information from each beneficial owner: • Name • Address • Date of birth • Driver's licence number and expiry date • Passport number and expiry date (English translations must be provided for foreign documents)	Electronic search Or Certified copy of current driver's licence and passport with English translations to verify the individual's: • Name; and • Address ***or*** date of birth

Unincorporated Association Identification and Verification

Identification – collect from the partnership:	**Verification – verify from reliable and independent documentation or electronic data**
Full name of the association	Minimum due diligence (in order of preference): • Partnership agreement; or • Certified copy or certified extract from the partnership agreement
Full address of the principal place of administration (if any)	**Not required** for minimum due diligence
Full name of the chairman, secretary and treasurer or equivalent officer in each case of the association	**Not required** for minimum due diligence
In respect of a member – the information required to be collected from an individual under the applicable customer identification procedure with respect to individuals	Minimum due diligence is the verification procedures relating to individuals
The following information from each beneficial owner: • Name • Address • Date of birth • Driver's licence number and expiry date • Passport number and expiry date (English translations must be provided for foreign documents)	Electronic search Or Certified copy of current driver's licence and passport with English translations to verify the individual's: • Name; and • Address ***or*** date of birth

Ongoing Customer Due Diligence

When completing ongoing customer due diligence, you must:

- update the KYC Information held on file in respect of relevant parties to a transaction;
- assess the on-going reputational risk of the transaction to NAIF; and
- determine if any additional KYC Information is required to be obtained in respect of a party to the transaction depending upon the risk assessment of the transaction.

Attachment 2 – NAIF Transaction Risk Assessment (TRA) Form

Customer

Full legal name of customer	Address/ Registered address	Company search	Dow Jones search	Google search

Parties Relevant to the transaction

Full legal name of Party	Relevance to transaction	Address/ Registered address	Dow Jones search	Google search

AML/CTF KYC Collection and Verification

Please insert relevant table from Attachment 1 of the Procedures. (An example for an Australian proprietary company is set out below.)

Identification	Collection	Verification
Full name of the company		
Full address of the company's registered office		
Full address of the company's principal place of business (if different)		
ACN		
Whether it is registered as a proprietary or public company		
The name of each director		
The following information for each beneficial owner: • Name • Address • Date of birth • Driver's licence number and expiry date • Passport number and expiry date		

ML/TF Risk Assessment

Customer

Provide written commentary on each relevant customer, its control structure, history, ownership (including beneficial owners), related parties, any known incidents associated with it or related companies etc.

PEPs

The following PEPs are associated with the customer or entities associated with the customer:

Name	DOB	Address	Nature of PEP	Association with customer	Association with another entity

Industry

Provide written commentary on the industry/ ies each relevant customer and its related companies operate in, including any other source of funds and wealth, and any MLTF/Risks or reputational risks that might arise.

Nature and purpose of business relationship

Provide written commentary on the nature and purpose of NAIF's business relationship, or proposed business relationship, with each relevant customer.

Jurisdiction

Provide written commentary on jurisdiction of each relevant customer (generally registered address of the company and the jurisdiction or residence of the customer's beneficial owners).

In addition provide written commentary on the jurisdictions of other parties associated with the whole transaction such as:

- owners and beneficial owners of the project proponent
- joint venture partners in any special purpose vehicle (SPV) used to develop the project
- subcontractors to the project
- suppliers to the project
- agents of the project
- off-takers of any end product of the project

Products and Services

Provision of a [loan/guarantee] which is considered low residual risk.

Delivery Channel

Direct delivery channel as evidenced by:

- Face to face meetings with a project proponent
- Direct emails, correspondence and telephone calls from representatives of the project proponent
- Site visits to the proposed project site.

ML/TF Risk Analysis and Rating

Please rate the customer as either high, medium or low risk:

	Rating Criteria	**Risk Rating**
Low Risk Customer	Customer does not meet any of the High or Medium risk criteria below.	
Medium Risk Customer	Customer: • with one or more beneficial owners in a medium jurisdiction; or • undertaking moderately high risk business activities.	
High Risk Customer	Customer: • with a complex ownership structure; • associated with one or more PEPs; • with one or more beneficial owners in a high risk jurisdiction; or • undertaking very high risk business activities.	

Provide written commentary on the ML/TF Risk associated with the customer, taking into account the written commentary above on:

- the customer,
- the customer's beneficial owners,
- any PEPs associated with the customer,
- the customer's source of funds and wealth, including the customer's industry,
- each relevant jurisdiction,
- the product
- the delivery channel

Supplementary KYC Collection and Verification

Only required where the risk has been assessed as “high” or “very high”. Provide additional KYC information and written commentary on how the additional KYC information (or other steps, including verification of information beyond the minimum due diligence requirements) addresses the assessed ML/TF risk.

Transaction Risk Analysis and Recommendation

Please rate the transaction as either high, medium or low risk:

	Rating Criteria	Risk Rating
Low Risk	The transaction does not meet any of the High or Medium risk criteria below.	
Medium Risk	The transaction: • involves one or more customers rated as medium risk; or • has some political or reputational risk attached to it.	
High Risk	The transaction: • involves one or more customers rated as high risk; or • has significant political or reputational risk attached to it.	

Provide written commentary on the risks of the transaction with an overview of ML/TF Risks and key reputational risks relating to the transaction as a whole, not just the relationship with a particular risk party.

Such risk factors can arise from information obtained through conducting searches or otherwise (for example from press reports.) The analysis should include commentary on the results of the searches and include information about incidents or adverse media reports contained in Dow Jones and Google searches that have taken place during the last 10 years.