



Financial Analysis and Supervision Unit

Guidance for Reporting Entities to Raise Awareness on Record Keeping under the *Anti-Money Laundering and Counter Terrorist Financing Act 2015* (No. 6 of 2025)

Issued by the Financial Analysis and Supervision Unit on 26th of September 2025

Disclaimer: This Guidance is issued in accordance with Section 72(1)(b),(2)(b) of the *Anti-Money Laundering and Counter Terrorist Financing Act 2015* (Act) for awareness raising purposes only and cannot be relied on as evidence of complying with the obligations of the Act. It does not constitute legal advice and cannot be relied on as such. Nor is it intended to be guidance for the purposes of a Compliance Rule under Sections 73 and 74 of the Act. After reading this Guidance, if you do not fully understand your obligations or have any questions, you should contact the Financial Analysis and Supervision Unit on email fasu@bankpng.gov.pg or telephone number +675 322 7147.

Document Version Control

Version	Date Issued	Document Status	Document Author
1	06.08.25	Draft	Asian Development Bank Consultant
2	21.08.25	Draft	FASU
3	30.08.25	Draft	Asian Development Bank Consultant
4	26.09.25	Final	FASU

Table of Contents

TABLE OF ACRONYMS3

1. KEY CONCEPTS AND TERMS4

2. NOTE TO READING THIS GUIDANCE7

3. REQUIREMENTS UNDER THE ACT.....9

4. RECORD KEEPING.....10

4.1. WHAT RECORDS MUST BE KEPT? 10

4.2. HOW SHOULD THE RECORDS BE KEPT? 12

4.3. HOW LONG MUST RECORDS BE KEPT?..... 12

4.4. WHERE SHOULD RECORDS BE KEPT? 12

REFERENCES AND CONTACTS.....14

Table of Acronyms

Act	Anti-Money Laundering and Countering Terrorist Financing Act 2015
AML/CTF	Anti-Money Laundering/Counter Terrorist Financing
CDD	Customer (or Client) Due Diligence
DNFBPs	Designated Non-Financial Businesses or Professions
ECDD	Enhanced Customer Due Diligence
FASU	Financial Analysis and Supervision Unit
FATF	Financial Action Task Force
ID	Identification
ML	Money Laundering
RBA	Risk-based Approach
SMR	Suspicious Matter Report
TF/FT	Terrorist Financing/Financing of Terrorism
UNFSA	United Nations Financial Sanctions Act 2015

1. Key Concepts and Terms



A number of terms used in this Guidance are defined in Section 5 of the Act. You must rely on the technical definitions of these terms as stipulated in the Act. Only for the purpose of assisting reporting entities in understanding their obligations, this Guidance provides a lay explanation of some of these key terms above.

- 1.1. **Beneficial Owner** in the context of **legal persons**, refers to the natural person(s) who ultimately owns¹ or controls², directly or indirectly, a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those natural persons who exercise ultimate effective control over a legal person. Only a natural person can be an ultimate beneficial owner, and more than one natural person can be the ultimate beneficial owner of a given legal person.

In the context of **legal arrangements**, beneficial owner includes: (i) the settlor(s); (ii) the trustee(s); (iii) the protector(s) (if any); (iv) each beneficiary, or where applicable, the class of beneficiaries and objects of a power; and (v) any other natural person(s) exercising ultimate effective control over the arrangement. In the case of a legal arrangement similar to an express trust, beneficial owner refers to the natural person(s) holding an equivalent position to those referred to above. When the trustee and any other party to the legal arrangement is a legal person, the beneficial owner of that legal person should be identified.

- 1.2. **Customer (or client)** as defined in Section 5 of the Act means a customer, person³ or unincorporated entity for whom a reporting entity carries out a transaction; or with whom a reporting entity conducts a business relationship, and includes such people or entities who/that attempt to carry out a transaction or business relationship, as well as a new or existing client.
- 1.3. **Customer Due Diligence (CDD)** is, at a minimum, the process of:
- a). identifying a customer and ensuring that they are who they claim to be, i.e. verifying the customer;
 - b). maintaining current and up to date information and records relating to the customer and (where relevant) their beneficial owners, and the nature and purpose of the business relationship, and the customer's commercial or personal activities; and
 - c). ensuring that transactions carried out on behalf of a customer are consistent with the financial institution's knowledge of the customer, the customer's commercial or personal activities and risk profile, and where necessary, the source of the funds.
- 1.4. **Designated Non-Financial Businesses or Professions (DNFBPs)**, as defined in Section 5 of the [Anti-Money Laundering and Combating Terrorist Financing Act 2015](#) (hereinafter referred to as "Act"), includes a casino, real estate agent, dealer in precious metals or precious stones,

¹ "Owns" means ownership, either directly or indirectly, of 25% or more of a person or unincorporated entity.

² "Control" includes control as a result of, or by means of, trusts, agreements, arrangements, understandings and practices, whether or not having legal or equitable force and whether or not based on legal or equitable rights, and includes exercising control through the capacity to make decisions about financial and operating policies.

³ Person as defined under Section 5 of the Act means a natural person and a body corporate.

lawyers, notary public, other independent legal professionals and an accountant when undertaking certain transactions on behalf of a client, a trust or company service provider, and a motor vehicle dealer.

- 1.5. **Financial Analysis and Supervision Unit (FASU)** is established under Section 61 of the Act whose functions are set out in Section 72(1)(2)(3) of the Act which are to:
- 1.5.1. carry out financial intelligence and analysis concerning suspected money laundering and associated predicate offences, terrorist financing and proceeds of crime;
 - 1.5.2. monitor and enforce compliance with the Act; and
 - 1.5.3. receive reports and information provided to it under PNG's proceeds of crime law and disseminate such reports and information in accordance with PNG's proceeds of crime law and the Act.
- 1.6. **Financial Institutions (FIs)**, as defined in Section 5 of Act, includes a commercial bank, micro bank, finance company, savings and loans society, insurance company, insurance agency and broker, brokerage firm, superannuation fund, leasing company, funds management company and money changer.
- 1.7. **Money Laundering (ML)** is the process of hiding the illegal origin of money and making it appear to come from legitimate sources. It usually happens in three stages: (1) Placement – putting the illegal money into the financial system, (2) Layering – moving it around through different transactions to hide its origin, and (3) Integration – bringing it back into the economy as “clean” money that appears to have come from a legitimate source.
- 1.8. **Politically Exposed Person (PEP)**, as defined in Section 5 of the Act, means a person who has been entrusted with prominent public functions in PNG or another country, and an immediate family member or close associate of that person.
- 1.9. **Proliferation Financing (PF)** is the act of providing funds or financial services which are used, whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biochemical weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.
- 1.10. **Record** means information recorded or retained in any form which can be accessed in or from PNG and which can be read or understood by a person, computer system or other device.
- 1.11. **Reporting Entity** means financial institutions and DNFBPs that have a legal requirement to comply with the Act and includes entities that are required to be registered with FASU pursuant to Section 57 of the Act.
- 1.12. **Risk** occurs when a threat successfully takes advantage of a vulnerability to produce a consequence. Simply, risk in the context of money laundering (ML) and terrorist financing (TF) can be seen as a function of three factors: threat, vulnerability, and consequence.

- a). **threat** is a person or group, object or activity with the potential to cause harm to the state, society or the economy. In the context of ML/TF, 'threat' includes criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities
 - b). **vulnerability** refers to those characteristics of a business that can be exploited by the threat or that may support or facilitate its activities. This includes features of a particular sector that can be exploited, such as customer types, products and services, delivery channels and the foreign jurisdictions with which it deals. Vulnerability is also influenced by the AML/CTF systems and controls in place by the business
 - c). **consequence** refers to the potential impact or harm that ML/TF activity may cause if it materialises and includes the effect of the underlying criminal activity or terrorist on you and your business or profession.
 - d). **likelihood** of a risk manifesting is based on the combined assessment of the **threat** to and **vulnerability** of your business or profession to ML and TF activity.
- I.13. **Risk Assessment** is the process of identifying, analysing and evaluating, and mitigating and managing risks.
- I.14. **Terrorist Financing (TF)** is providing or collecting property to finance terrorist activities, individual terrorists or terrorist organisations.

2. Note to Reading this Guidance



This Guidance intends to raise awareness to reporting entities on the requirements of the Act and relevant international standards set by FATF. It is not legal advice, and as such, does not intend to replace the Act.

- 2.1. This Guidance is developed in accordance with Section 72(1)(b),(2)(b) of the *Anti-Money Laundering and Counter Terrorist Financing Act 2015* (hereinafter referred to as 'Act') to raise awareness of money laundering and terrorist financing and obligations on financial institutions (FIs) and designated non-financial businesses or professions (DNFBPs).
- 2.2. This Guidance applies to both FIs and DNFBPs (hereafter jointly referred to as 'reporting entities').
- 2.3. This Guidance aims to support and enhance reporting entities' understanding and implementation of record-keeping requirements outlined in the Act.
- 2.4. Record keeping is an essential component of the audit trail that the Act seeks to establish to assist in any financial investigations and to ensure that criminal funds are kept out of the financial system, or if not, that they may be detected and confiscated. These obligations are important to ensure that in investigations or prosecutions involving money laundering (ML) and terrorist financing (TF), evidence of a particular transaction or business can readily be made available.
- 2.5. Reporting entities must also retain the required records concerning customer identification and transactions to demonstrate that they are complying with their obligations, and FASU has the power to seek production of any records under the Act for supervision and enforcement purposes.
- 2.6. This Guidance is not law, but it can be used side by side with current laws of the PNG and as a reference for the interpretation and implementation of existing anti-money laundering and counter terrorist financing (AML/CTF) legislative requirements which apply to reporting entities in PNG. The Guidance should be read in conjunction with the following FASU Guidance below, which are available on the website of the Bank of PNG:
 - a). [Guidance for Financial Institutions on their Obligations under the Anti-Money Laundering and Counter Terrorist Financing Act 2015 \(No. 1 of 2019\) \(issued on 20 May 2019\)](#);
 - b). [Guidance for Designated Non-Financial Businesses or Professions on their Obligations under the Anti-Money Laundering and Counter Terrorist Financing Act 2015 \(No. 2 of 2019\) \(issued on 20 May 2019\)](#); and
 - c). [Guidance on Supervision and Enforcement Powers of the Financial Analysis and Supervision Unit under the Anti-Money Laundering and Counter Terrorist Financing Act 2015 \(No. 3 of 2019\)](#).
- 2.7. This Guidance intends to provide industry guidance, practical assistance and a means for reporting entities to better comply with their AML/CTF obligations under the Act.

- 2.8. For ease of reference, in each Section, where appropriate, you will also find references to the relevant provisions of the [Act](#) and cross-references to [other related Guidelines](#).
- 2.9. Reporting entities should develop their own AML/CTF internal policies, procedures and controls tailored to their business needs.
- 2.10. Some of the ‘marks’ used in the textboxes of this Guidance should be read as below:

<i>i</i>	Textbox in this format provides information to assist reporting entities understand their obligations and the provisions in the Act to which those obligations relate.
<i>e.g.</i>	Textbox in this format provides appropriate examples.
!	Textbox in this format stresses important information for reporting entities, including on penalties for non-compliance with obligations under the Act.

3. Requirements under the Act

- 3.1. The international recommendations and the AML/CTF laws of PNG outline ways that are proven to help deter and detect instances of ML and TF. These all form the basis of your AML/CTF obligations and the requirements which must be followed and implemented by a reporting entity, including the record-keeping obligations.



The Act sets out the record keeping obligations in Part II, Division 4 (Sections 47 to 51). These obligations apply to both financial institutions and DNFBPs.

- 3.2. The Act requires reporting entities to maintain different types of records, including transaction records, identity and verification of customer records, records relating to risk assessments, AML/CTF program and audits, and other customer-related records, such as account files and business correspondence (more details provided under [Record Keeping](#) of this Guidance).



Failure to comply with the record-keeping obligations is a crime punishable by up to 5 years imprisonment, and fines of K500,000 for an individual and K1,000,000 for a body corporate (Section 51).

- 3.3. Reporting entities are obliged to comply with FASU's request, in writing, to produce records, maintained under the Act, in their possession. FASU may also specify the manner in which and a reasonable period within which records are to be provided.
- 3.4. Failure to comply with FASU's request to produce records is an offence under the Act.

4. Record Keeping

4.1. What records must be kept?

4.1.1. All reporting entities must comply with the record-keeping requirements outlined within the Act. The documents you are required to keep, range from CDD-related documents to other more general transactional and financial records. Ultimately, you must ensure you keep and maintain all necessary records and transactions relative to your dealings with your customers.

4.1.2. The types of records reporting entities are required to keep are:

- 4.1.2.1. Records of all transactions, including occasional transactions, carried out with or for your customers, including sufficient supporting documents (consisting of original documents or copies) in respect of a transaction;
- 4.1.2.2. CDD measures carried out on customers, including a copy of any documents and information obtained by you to satisfy CDD requirements under the Act;
- 4.1.2.3. Other customer records, such as account files or business correspondence obtained during the establishment or throughout the course of the business relationship, including the results of any analysis undertaken (e.g., inquiries to establish the background and purpose of transactions);
- 4.1.2.4. Records of internal risk assessment, AML/CFT program, and audits undertaken of AML/CTF controls, including any reports made by the compliance officer to senior management;
- 4.1.2.5. Copies of all “internal” SMRs made to the compliance officer, and any investigations undertaken; and
- 4.1.2.6. Copies of all “external” SMRs made to the FASU; and
- 4.1.2.7. Details of any AML/CTF training completed, including dates of training sessions, description of training provided, and name of employees who attended the training.

4.1.3. More specifically, reporting entities shall keep:

4.1.3.1. Institutional/Organisational records

All reporting entities must ensure that they keep records that show the purpose, objectives and activities of their institution/business/professions; the identity of people who control or direct its activities including board members, directors and managers.

4.1.3.2. Due diligence – Identity and verification records

Where the reporting entity has undertaken due diligence on a customer, they must ensure that they keep a record of this due diligence, including any evidence used to identify and verify the customer. CDD and ECDD are integral to an effective functioning of AML/CTF regime. Therefore, it is important that all records are kept in a manner that allows you, as a reporting entity, to maintain active oversight in the case of ongoing business relationships.

4.1.3.3. Transaction records

All transactions carried out on behalf of or with a customer in the course of relevant business must be recorded

Records of transactions undertaken by the reporting entities must include the following details:

- a) customer's name and address;
- b) the beneficiary of the transaction (as well as their name and address);
- c) date of transaction;
- d) nature of transaction;
- e) the amount of the transaction and the types of currency;
- f) the account details with the financial institution involved in the transaction including account number, name and identifier;
- g) the name and address of the financial institution and name of the officer, employee or agent of the financial institution who handled the transaction, if that officer, employee or agent - (i) has face-to-face dealings in respect of the transaction with any of the parties to the transaction; and (ii) has formed a suspicion under Section 41(1); and
- h) any relevant files and correspondence in relation to the transaction.

Any records you keep on a transaction must be sufficiently detailed enough, in accordance with the requirements of the Act, so that the transaction could be understood, if reviewed, and permits the reconstruction of individual transactions.

Additionally, the records must be able to show and explain the reporting entity's transactions, within and outside of the territory.

4.1.3.4. Internal and external reports

Reporting entities shall keep and maintain:

- a) records of all "internal" suspicious activity or transaction reports made by employees to the compliance officer, and any investigations or action taken, including record of any material, information or documents that was considered by the compliance officer to take a decision; and
- b) records of all "external" SMRs filed to the FASU

4.1.3.5. Training and compliance monitoring

Reporting entities shall maintain the following records:

- a) In relation to AML/CFT training:
 - the date any training was given;
 - the names of the attendees;
 - the duration of the training;
 - the topics covered in the training;

- where appropriate, the results of the tests undertaken by employees
- b) In relation to compliance monitoring:
 - reports by the compliance officer to senior management; and
 - records of consideration of those reports and of any action taken as a consequence.

4.1.3.6. Reporting entities are required document and maintain records of their **internal risk assessment reports, AML/CFT program** and **audits** (internal and external) undertaken to determine the effectiveness of their AML/CFT controls, include any recommendations made and actions taken.

4.2. How should the records be kept?

- 4.2.1. As a reporting entity, you must ensure that you keep records in an easily retrievable format, which by extension means that the records must be kept in an orderly, sensible manner so that the records and the information in the records can be easily searched, and produced without delay, if required.
- 4.2.2. Records may be kept:
- 4.2.2.1. as original documents;
 - 4.2.2.2. as original copies or certified copies of the original documents;
 - 4.2.2.3. as a scanned copy of the original document, which can be certified; or
 - 4.2.2.4. in a computerized or other electronic format.
- 4.2.3. It will be up to the reporting entities to decide how it chooses to store and keep these records. However, you must ensure that the criteria provided within the Act and covered above are included.

4.3. How long must records be kept?

- 4.3.1. Records must be kept for a **minimum of seven (7) years**. For transactions, the time period is seven (7) years after the completion of the last transaction or series of transactions, including occasional transaction. For business relationships, the time period is seven (7) years after the end of the business relationship.
- 4.3.2. In certain circumstances, FASU may ask you to keep records for a longer period than seven (7) years – the requirement you are obliged to comply with.

4.4. Where should records be kept?

- 4.4.1. The Act does not state where the relevant records should be kept but the overriding objective is for reporting entities to be able to retrieve relevant information without undue delay and make it available to FASU upon request.
- 4.4.2. Where records are held outside PNG, it is the responsibility of the reporting entity to ensure that the records available meet the requirements of the Act. No secrecy or data protection legislation should restrict access to the records either by the reporting entity or FASU. If it is

found that such restrictions exist, copies of the underlying records shall be sought and retained within PNG.

- 4.4.3. Reporting entities should take account of the scope of AML/CFT legislation in other countries, and should ensure that group records kept in other countries that are needed to comply with PNG law are retained for the required period.

References and Contacts

PNG's AML/CTF Framework

Information on the Act and PNG's regime can be found at www.bankpng.gov.pg

- PNG's *Anti-Money Laundering and Counter Terrorist Financing Act 2015*:
<https://www.bankpng.gov.pg/sites/default/files/2024-09/1-No-20-of-2015-Anti-Money-LaunderingCounter-Terrorist-Financing-Act-2015.pdf>
- PNG's *Criminal Code Act 1974*: http://www.paclii.org/pg/legis/consol_act/cca1974115/
- PNG's *Criminal Code (Money Laundering and Terrorist Financing) (Amendment) Act 2015*:
https://www.bankpng.gov.pg/sites/default/files/2024-09/No-21-of-2015-Criminal-Code-Money-Laundering-Terrorism-FinancingAmendment_Act-2015.pdf
- PNG's *Mutual Assistance in Criminal Matters (Amendment) Act 2015*:
<https://www.bankpng.gov.pg/sites/default/files/2024-09/No-22-of-2015-Mutual-Assistance-in-Criminal-Matters-Amendment-Act-2015.pdf>
- PNG's *Proceeds of Crime Act 2005*: http://www.paclii.org/pg/legis/consol_act/poca2005160/
- PNG's *Proceeds of Crime Act (Amendment) 2015*:
<https://www.bankpng.gov.pg/sites/default/files/2024-09/No-23-of-2015-Proceeds-of-Crime-Amendment-Act-20153.pdf>
- PNG's *United Nations Financial Sanctions Act 2015*:
<https://www.bankpng.gov.pg/sites/default/files/2024-09/No-24-of-2015-United-Nations-Financial-Sanctions-Act-20151.pdf>

Asia Pacific Group on Money Laundering (APG): <http://www.apgml.org>

Financial Action Task Force (FATF): <http://www.fatf-gafi.org>

For queries about this Guidance, please contact:

Bank of PNG, Financial Analysis and Supervision Unit

PO Box 121, Port Moresby, National Capital District

W: www.bankpng.gov.pg

E: fasu@bankpng.gov.pg

T: +675 322 7147