ENFORCEMENT AND INVESTOR PROTECTION DEPARTMENT
ANTI-MONEY LAUNDERING DIVISION

N O T I C E

TO: ALL SEC COVERED PERSONS

SUBJECT: RESULTS OF THE PHILIPPINES' 3RD NATIONAL RISK ASSESSMENT

The Philippines has completed its 3rd National Risk Assessment (NRA) on Money Laundering (ML), Terrorism Financing (TF), and Proliferation Financing (PF) for the covered period 2021 to 2024. The results of the risk assessment, along with the relevant Frequently Asked Questions (FAQs), are available on the Anti–Money Laundering Council's (AMLC's) website: http://www.amlc.gov.ph/publications/national-risk-assessment.

Covered Persons (CPs) are strongly encouraged to **incorporate the results** into their compliance programs, consistent with the risk-based approach prescribed under SEC Memorandum Circular No. 16 series of 2018. CPs should use the findings of the NRA to reassess and, where necessary, recalibrate their institutional risk assessments, customer risk profiling, and overall Money Laundering and Terrorism Financing Prevention Programs (MTPPs). This includes aligning customer due diligence measures, enhanced due diligence procedures, transaction monitoring systems, and internal controls with the identified national risk levels and priority threat areas.

By integrating the NRA results into their policies and procedures, CPs can better ensure that mitigating controls are proportionate to their inherent risks, strengthen their compliance framework, and demonstrate adherence to regulatory expectations on risk management, governance, and ongoing monitoring under the applicable AML/CFT/CPF regulations.

Attached to this Notice is a copy of the results of the 3rd Philippines' NRA.

ARCS-N-AMLCFT-2025-1

The Third National Risk Assessment (NRA) on Money Laundering, Terrorism Financing, and Proliferation Financing

Republic of the Philippines
2021-2024

Abridged Public Version

Table of Contents

Message from the NACC Chairman

Office of the President
Malacañang

MESSAGE

The **Third National Risk Assessment (NRA) on Money Laundering, Terrorism Financing, and Proliferation Financing** marks a decisive step in strengthening the Philippines' financial integrity framework. It is a clear and unequivocal statement of the Marcos, Jr. administration's resolve to protect our financial system, uphold institutional credibility, and secure the nation's economic future.

Our exit from the FATF grey list in February 2025 is a hard-earned achievement, but it is not a finish line. Financial crime evolves rapidly, driven by technology and sophistication. Complacency is not an option. Vigilance, innovation, and sustained political will must continuously define our response. That is why this Public Version of the NRA is a critical policy compass guiding the next National AML/CTF/CPF Strategy and shaping our legislative, regulatory, and enforcement agenda.

On behalf of the National AML/CTF/CPF Coordinating Committee (NACC), I commend the Anti-Money Laundering Council (AMLC), our regulators, law enforcement agencies, and private-sector partners for delivering this rigorous and forward-looking assessment. Their whole-of-nation effort reflects a shared and unwavering commitment to a transparent, secure, and trusted financial system.

Financial integrity is the foundation of our security, investor confidence, and a just and prosperous Philippines. We owe it to the Filipino people to ensure that our financial system is not hijacked by criminal enterprise, nor used as a conduit for the corrupt. Let this NRA be our continued commitment to build a financial system that protects the nation, upholds the rule of law, and ultimately, improves the lives of every Filipino.

For at the end of the day, every reform, every safeguard, every victory in this fight against financial crime must redound to one purpose: a better, safer, and more dignified life for every Filipino under Bagong Pilipinas.

RALPH G. RECTO
Executive Secretary
Chairman, National AML/CTF/CPF
Coordinating Committee

BAGONG PILIPINAS

Message from the BSP Governor and AMLC Chairman

BANGKO SENTRAL NG PILIPINAS

MESSAGE

The Third National Risk Assessment (NRA) offers a clear view of the Philippines' key risks related to money laundering, terrorism financing, and proliferation financing. It draws on insights from regulators, supervisors, and law enforcement agencies to guide both government and private sector stakeholders in strengthening safeguards for our financial system.

This report is a key reference for government and private sector stakeholders in understanding risks and designing effective, risk-based measures to protect the financial system.

With the rapid shift to digital finance, the NRA is more relevant than ever. It helps us identify vulnerabilities, reinforce coordination, and ensure that innovation is matched by strong risk management.

The Philippines' removal from the Financial Action Task Force grey list reflects our progress in addressing strategic deficiencies. The NRA builds on this momentum by highlighting both the gains achieved and the challenges ahead particularly in the banking sector and digital financial space.

The BSP, together with the Anti-Money Laundering Council, remains committed to risk-based supervision, improved financial intelligence, and close collaboration with our partners. These efforts are key to preserving trust and supporting sustainable, inclusive growth.

Eli M. Remolona, Jr.
Governor, Bangko Sentral ng Pilipinas
Chairman, Anti-Money Laundering Council

8811-1BSP (1277) bspmail@bsp.gov.ph bsp.gov.ph A. Mabini St. Malate 1004 Manila, Philippines

Message from SEC Chairman (AMLC Member)

MESSAGE

As our capital markets and corporate sector continue to grow in scale and complexity, our understanding of the risks that accompany this growth must deepen as well. The Third National Risk Assessment provides an important and timely lens into the vulnerabilities facing the corporate sector, capital markets, non-profit organizations, and designated non-financial businesses and professions.

The findings of the NRA strongly reinforce the direction we have taken at the Securities and Exchange Commission—promoting transparency, strengthening corporate governance, and advancing risk-based supervision. The emphasis on improving beneficial ownership information, preventing the misuse of corporate vehicles, strengthening oversight of NPOs, and enhancing monitoring of DNFBPs underscores a simple truth: market growth must be matched by discipline, accountability, and constant vigilance.

Our recent exit from the FATF grey list is a significant milestone and a source of renewed confidence. But it is not a finish line. The NRA highlights that emerging financial crime typologies – such as the misuse of corporate vehicles, evolving fundraising mechanisms, and vulnerabilities in certain professional service – require sustained vigilance and adaptive regulatory responses.

We commend the Anti-Money Laundering Council and all partner agencies for this comprehensive and forward-looking assessment. For the SEC, this serves not merely as a diagnostic, but as a call to sustained action. We remain fully committed to reforms that strengthen investor protection, uphold transparency, and ensure that our corporate and capital markets cannot be misused to undermine trust.

Francisco Ed. Lim
Chairman, Securities and Exchange Commission
Member, Anti-Money Laundering Council

Message from Insurance Commissioner (AMLC Member)

Republic of the Philippines
Department of Finance
INSURANCE COMMISSION
1071 United Nations Avenue, Manila

BAGONG PILIPINAS

MESSAGE

The insurance sector plays an increasingly important role in the Philippine financial system, making the understanding of its risk environment essential for strengthening resilience against money laundering, terrorism financing, and proliferation financing. The Third National Risk Assessment (NRA) offers valuable guidance for enhancing risk management practices across the industry at a time of expanding innovation and digital adoption.

The NRA reaffirms that the sector is comparatively low-risk, yet it also identifies areas requiring enhanced vigilance—such as investment-linked products, the role of intermediaries, sanctions compliance, and emerging digital vulnerabilities. These insights highlight the need for strong governance, continuous capacity-building, and a proactive approach to compliance.

Supported by broader reforms that contributed to the Philippines' exit from the FATF grey list, the Insurance Commission will continue strengthening risk-based supervision, expanding the use of data analytics, and supporting industry efforts to safeguard policyholders and maintain market confidence.

We express our gratitude to the AMLC, government partners, and industry stakeholders who contributed to this national assessment. The IC remains committed to supporting the implementation of the National AML/CTF/CPF Strategy and ensuring that the insurance industry contributes to a secure, transparent, and trusted financial system.

Atty. Reynaldo A. Regalado
Insurance Commissioner
Member, Anti-Money Laundering Council

Message from AMLC Executive Director

Republic of the Philippines
ANTI-MONEY LAUNDERING COUNCIL

BAGONG PILIPINAS

SECRETARIAT

MESSAGE

The Third National Risk Assessment (NRA) represents a significant advance in the Philippines' collective effort to understand and address the risks of money laundering, terrorism financing, and proliferation financing. As the most comprehensive assessment undertaken to date, it provides a robust analytical foundation for shaping the next generation of AML/CTF/CPF reforms and strengthening the country's preparedness for emerging financial crime threats.

This NRA draws upon a wide array of data sources—including suspicious transaction reports, supervisory findings, law enforcement intelligence, sectoral surveys, and international cooperation inputs—and integrates them through a structured methodology. We acknowledge with appreciation the World Bank for its technical support and the application of its NRA Tool, which enabled a systematic, data-driven evaluation of sectoral risks.

The findings reflect both the progress we have achieved and the challenges that remain. Significant improvements have been made in strengthening financial intelligence capabilities, enhancing supervision, increasing access to beneficial ownership information, and improving enforcement outcomes. At the same time, high-threat predicate crimes, vulnerabilities among certain DNFBPs and digital channels, and persistent capacity gaps in PF implementation require sustained focus and continued investment in institutional capability.

As the Philippines' Financial Intelligence Unit, the AMLC can leverage the findings in the NRA to strategically allocate its resources. These insights will enable the AMLC to concentrate its financial analysis and investigative efforts on high-threat crimes, while also strengthening its supervisory focus on industries and channels identified as highly vulnerable to criminal and terrorist activities.

The AMLC Secretariat extends its deep appreciation to all participating government agencies, supervisory authorities, law enforcement bodies, and private-sector partners for their engagement throughout this process. Their contributions were essential to producing an assessment that is both rigorous and forward-looking. The insights generated from this NRA will directly inform the development of the National AML/CTF/CPF Strategy 2026-2030, guiding our transition toward a more resilient, data-driven, and future-ready AML/CTF/CPF ecosystem.

As we enter the next cycle of reforms, the AMLC remains firmly committed to protecting the integrity of the Philippine financial system, safeguarding national security interests, and maintaining the trust and confidence of the global community.

Atty. Matthew M. David
Executive Director, Anti-Money Laundering Council Secretariat

File/Ref. No. AMLCS-OED-RADCS-25-___
Room 507, 5/F, EDPC Building, Bangko Sentral ng Pilipinas Complex, Malate, Manila, Philippines
Tel.No.: (+632) 8708-70-66; Fax No.: (+632) 8708-79-09 • www.amlc.gov.ph • secretariat@amlc.gov.ph

Foreword

The Third National Risk Assessment (NRA) on Money Laundering (ML), Terrorism Financing (TF), and Proliferation Financing (PF) presents the Philippines' updated view of its financial crime risks for the period 2021–2024. It is the most comprehensive assessment undertaken to date and the first to include a dedicated PF National Risk Assessment.

This NRA comes at an important time. In February 2025, the Financial Action Task Force (FATF) removed the Philippines from its "grey list" of jurisdictions under increased monitoring, following an on-site visit in January 2025. The FATF recognized substantial progress in addressing strategic deficiencies, including stronger supervision of high-risk sectors, improved access to beneficial ownership information, intensified enforcement, and measures to mitigate risks in casinos, money service businesses, non-profit organizations, and cross-border movements of cash.

The NRA underpins these achievements. It provides the analytical foundation for the National AML/CTF/CPF Strategy (NACS) and related action plans, and guides risk-based supervision, enforcement, and policy reform. It also responds to FATF Recommendation 1 and to evolving international expectations to assess not only ML and TF, but also PF risk.

The assessment was prepared under the leadership of the National AML/CTF/CPF Coordinating Committee (NACC) and its technical working groups, with broad participation from government agencies, regulators, law enforcement, the financial sector, designated non-financial businesses and professions (DNFBPs), and civil society. It draws on extensive data, cross-border cooperation, and international inputs, including a survey of 33 foreign Financial Intelligence Units (FIUs) on their experience of Philippine-linked ML and TF cases.

Going forward, this public version of the Third NRA is intended to:

- Inform policymakers, supervisors, and law enforcement agencies as they prioritize resources and reforms;
- Guide financial institutions, DNFBPs, and other covered persons in strengthening their own risk assessments and controls; and
- Demonstrate to international partners the Philippines' sustained commitment to transparency, integrity, and security in the financial system.

The government remains committed to sustaining and deepening reforms beyond the country's exit from the FATF grey list. The risks identified in this NRA—particularly around high-impact predicate crimes, cross-border channels, and emerging technologies—will continue to shape the agenda for the coming years.

Executive Summary

The Third National Risk Assessment (NRA) on Money Laundering (ML), Terrorism Financing (TF), and Proliferation Financing (PF) provides the Philippines' most comprehensive assessment of its financial crime risk landscape to date. Conducted after the Philippines' successful exit from the FATF grey list in February 2025, the NRA examines how the risk profile has evolved amid reforms, emerging technologies, and shifting criminal typologies.

This NRA covers the years 2021–2024 and incorporates, for the first time, a full Proliferation Financing National Risk Assessment, consistent with updated FATF Standards. It draws on inputs from regulators, law enforcement agencies, the financial sector, DNFBPs, non-profit organizations, foreign FIUs, and civil society. The assessment is anchored in the World Bank ML/TF NRA Toolkit for ML and TF risks, and a dedicated methodology aligned with FATF Recommendation (Rec.) 1 in relation to Rec. 7 for PF.

The findings of this NRA will inform the National AML/CTF/CPF Strategy (2026–2030) and help guide risk-based supervision, policy development, and enforcement priorities across all sectors.

Scope and Approach

The **Third National Risk Assessment (2021–2024)** evaluates the country's exposure to:

- **Money Laundering (ML);**
- **Terrorism Financing (TF);** and
- **Proliferation Financing (PF)**—through the Philippines' first dedicated PF National Risk Assessment covering 2019–2023.

For ML and TF, the assessment applies the **World Bank National ML/TF Risk Assessment Toolkit**, incorporating modules on national vulnerability and sectoral vulnerabilities across banking, securities, insurance, DNFBPs, and other financial institutions. For PF, a tailored methodology was developed in line with **FATF Recommendation 1**, in relation to **Recommendation 7** and relevant **UN Security Council Resolutions**, leveraging insights from the country's new PF NRA.

The ML/TF assessment period spans **2021–2024**, drawing on:

- Suspicious and covered transaction reports (STRs/CTRs);
- Investigation, prosecution, and asset recovery data;
- Supervisory findings and sanctions;
- Sectoral surveys and institutional risk assessments; and
- Cross-border intelligence and an international FIU survey

Overall National Risk Levels

At a strategic level, the NRA concludes:

- **National ML Threat: High**
  Several predicate crimes generate significant illicit proceeds, notably drug trafficking, fraud, environmental crimes, and tax crimes.

- **National ML Vulnerability: Medium**
  The overall vulnerability score is **0.51 on a 0–1 scale**, reflecting moderate vulnerability after accounting for strengthened laws, institutions, and controls.

- **Overall ML Risk: Medium–High**
  The Philippines faces substantial domestic ML threats. While reforms have reduced vulnerabilities, they remain. National ML-combating capacity improved to **0.67**, driven by enhanced supervision, better access to beneficial ownership data, stronger enforcement, and coordinated national action.

- **TF Risk: Medium**
  TF risk has moderated since the previous cycle due to weakened domestic terrorist groups, improved intelligence coordination, stricter TF controls, and increased oversight of NPOs. However, risks persist in certain Mindanao provinces and remittance channels.

- **PF Risk: Medium**
  Although the Philippines has limited direct exposure to PF-designated jurisdictions, vulnerabilities remain due to uneven PF awareness, gaps in sanctions implementation, and the need for stronger controls among trade/logistics actors and certain covered institutions.

Key Messages

1. **A small number of predicate crimes dominate the ML threat.**
   Illegal drug trafficking, fraud (including cyber-enabled fraud), environmental crimes, and tax crimes pose high ML threats. Corruption and bribery, securities fraud, online sexual abuse and exploitation of children (OSAEC), and kidnapping for ransom are assessed as medium-high.

2. **Banks are central but relatively well controlled; other sectors show higher vulnerabilities.**
   - Banks hold the largest share of financial assets and formal financial flows. Their post-control ML vulnerability is **medium**, reflecting strong supervision and controls despite high inherent risks.
   - Casinos, real estate developers and brokers, money service businesses (MSBs), and virtual asset service providers (VASPs) exhibit higher inherent and residual vulnerabilities.

3. **Cross-border ML/TF risk is elevated, but concentrated in specific corridors and typologies.**
   Cross-border ML/TF risk is elevated but remains concentrated in a limited set of corridors and recurring typologies. International FIU feedback generally views the Philippines as a low-priority source or destination of illicit funds, with none of the surveyed jurisdictions rating it as a high ML/TF threat. Domestic indicators, however, assess the cross-border ML threat as High, reflecting increasing STR volumes and repeated cross-border flows linked to major predicate crimes and the expanding use of digital, remittance, and virtual asset channels—particularly in Southeast/East Asia-linked corridors and selected regional financial centers. Overall, cross-border ML risk is rated Medium-High (high threat moderated by medium vulnerability), underscoring the need to sustain cross-border transaction monitoring, apply sharper risk-based scrutiny to remittance and virtual asset channels, and deepen operational cooperation with foreign FIUs to trace and recover illicit proceeds across jurisdictions.

4. **Digital channels are a fast-growing risk vector.**
   Rapid adoption of e-money, remote onboarding, online remittances, and early-stage virtual asset activity has advanced financial inclusion but introduced new ML/TF/PF risks, including money mule schemes, account takeovers, and cross-border VA transfers. EMI-NBFIs show medium-high inherent vulnerability alongside a still-maturing control environment, while VASPs exhibit high inherent vulnerability; supervisory and industry controls are strengthening but remain in a maturation phase.

5. **National ML-combating ability has improved, but vulnerabilities persist—including in legal persons and arrangements.**
   The country's ML-combating score increased to 0.67 (Medium-High) from 0.60 in the 2nd NRA, reflecting stronger AML laws, a more active FIU, improved supervision, and more frequent asset freezing and forfeiture. Nonetheless, the informal economy, variations in STR quality.

   At the same time, transparency for legal persons has strengthened through higher-quality SEC registry controls, digitized filing/BO declaration processes, and improved access for competent authorities via data-sharing arrangements (with 69% of registered corporations compliant as of 31 December 2024); however, key gaps remain—particularly the absence of a well-defined BO disclosure mechanism for partnerships and trust arrangements, and residual constraints in BO quality as reflected in medium CDD-derived BO information—alongside enduring cross-cutting challenges such as the informal/cash economy and uneven financial intelligence/STR quality.

6. **TF risk has declined but remains concentrated in specific areas and channels.**
   While overall TF incidents are fewer, residual risk persists in conflict-affected areas—especially in Mindanao—where financing commonly involves small-value donations and community support moved through remittance and cash-based channels. The NPO sectoral assessment notes documented cases of targeted misuse of NPOs for fundraising, recruitment, and logistical support, with vulnerabilities heightened where NPOs rely heavily on cash and have limited oversight of volunteers and beneficiaries. Accordingly,

the NPO sector's residual TF risk is assessed as Medium, reinforcing the need for focused, proportionate, risk-based safeguards that concentrate on at-risk/high-risk NPOs operating in vulnerable regions or handling significant cash flows.

7. **PF is an emerging focus: threat is low, vulnerability is moderate.** The Philippines has limited trade and financial links with PF high-risk jurisdictions. Yet awareness of PF obligations is uneven, particularly among non-financial actors in trade, logistics, and export controls; PF-specific policies and controls are still being embedded.

8. **Financial inclusion products are low to medium risk when properly designed and supervised.**
   Microfinance, basic deposit accounts, microinsurance, and pawning remain low risk, while pawnshop remittances and basic e-money wallets are assessed as medium risk due to scale and exposure to fraud and other predicate crimes. Tiered CDD and transaction limits are critical mitigants.

9. **Philippines' exit from the FATF grey list is a milestone, not an endpoint.** Grey list exit in 2025 reduced frictions in cross-border transactions and strengthened investor confidence. However, reforms that supported delisting must be sustained and deepened, particularly in higher-risk sectors and PF implementation.

I. Country and System Context

Economic and Financial Landscape

The Philippines is a **lower-middle-income economy** and among the fastest-growing in Southeast Asia. By 2024, **GDP was estimated at approximately USD 460 billion**, driven primarily by services—including retail trade, business process outsourcing (BPO), tourism, and financial services—alongside manufacturing, construction, and remittances from **Overseas Filipino Workers (OFWs)**.

Banks dominate the financial system, accounting for more than four-fifths of total financial assets, with aggregate assets exceeding the country's GDP. Banks operate a nationwide network of over **13,000 offices**, serving as the backbone for payments, credit, and savings.

Other significant financial sectors include:

- **Money Service Businesses (MSBs):** Stand-alone remittance companies and money changers/FX dealers, operating thousands of branches nationwide and providing cash-intensive remittance and foreign exchange services.
- **Pawnshops:** Over **1,000 operators with more than 15,000 outlets**, widely used for short-term credit, remittances, and small-value foreign exchange transactions.
- **Electronic Money Issuers – Non-Bank Financial Institutions (EMI-NBFIs):** Over **40 licensed entities** offering e-wallets and digital payment services, which have grown rapidly in both volume and value.

- **Non-Stock Savings and Loan Associations (NSSLAs):** Closed membership institutions providing basic savings and loans to defined groups such as government employees and military personnel.
- **Trust Entities and Trust Corporations:** Managing significant assets under management across bespoke trusts, investment management accounts, and unit investment trust funds.
- **Operators of Payment Systems (OPS):** Nearly **300 entities** supporting clearing, settlement, merchant acquiring, bill payments, cash-in services, and network operations—forming the backbone of the digital payments ecosystem.
- **Securities and Insurance Sectors:** Smaller in overall balance sheet terms but critical for investment, savings, and long-term financial products.

Designated Non-Financial Businesses and Professions (DNFBPs) include casinos and online gaming operators, real estate developers and brokers, dealers in precious metals and stones, lawyers, accountants, and company service providers. Casinos and real estate, in particular, handle high-value domestic and cross-border transactions and feature prominently in ML typologies.

Digital Finance and Financial Inclusion

Account ownership increased significantly between 2019 and 2021, driven by **e-money adoption and digital banking**. More than half of adult Filipinos now hold a transactional account, primarily used for payments. **E-money transactions account for a large and growing share of retail payments**, with digital payments already representing more than half of retail transaction value and volume.

Financial inclusion products—such as **microfinance, basic deposit accounts, microinsurance, pawning, pawnshop remittances, and basic e-money wallets—are central to this trend**. Their design (small amounts, capped balances, limited functionality) and proportionate **Customer Due Diligence (CDD)** help contain ML/TF/PF risks. However, **remittance services and basic wallets remain vulnerable to fraud and mule activity if controls are weak**.

Governance and Institutional Arrangements

The country's AML/CTF/CPF framework is anchored in:

- **The Anti-Money Laundering Act of 2001 (AMLA), as amended**, including provisions on ML as a stand-alone offense, expanded predicates (including tax crimes and PF), reporting obligations, and targeted financial sanctions (TFS).

- **The Terrorism Financing Prevention and Suppression Act of 2012 (TFPSA)** and the Anti-Terrorism Act, which underpin TF criminalization, freezing mechanisms, and terrorist designation.

- **The Anti-Terrorism Act of 2020 (ATA)** defines and penalizes terrorism and related offenses, establishes the Anti-Terrorism Council (ATC), and enables terrorist designation

(including in line with UNSCR 1373) that triggers AMLC sanctions freeze orders against the funds and property of designated terrorists.

- **The Strategic Trade Management Act (STMA)** and related issuances, which provide the basis for controls on strategic goods and services relevant to PF.

At the institutional level:

- The **National AML/CTF/CPF Coordinating Committee (NACC)**, chaired at a high level, provides overall policy direction and inter-agency coordination.

- **The Anti-Money Laundering Council (AMLC)** is the Philippines' hybrid Financial Intelligence Unit (FIU) and the **primary implementer of the Anti-Money Laundering Act (AMLA)**, responsible for receiving and analyzing transaction reports and supervising non-prudentially regulated covered persons (including selected DNFBPs) for AML/CTF/CPF compliance.
- The **Bangko Sentral ng Pilipinas (BSP)** supervises banks, MSBs, EMI-NBFIs, OPS, and selected trust entities for both prudential and AML/CTF/CPF purposes.

- The **Securities and Exchange Commission (SEC)** oversees securities intermediaries, publicly listed companies, certain DNFBPs, and NPOs.

- The **Insurance Commission (IC)** supervises life and non-life insurers, pre-need companies, and related intermediaries.

- The **Philippine Amusement and Gaming Corporation (PAGCOR)** supervises and regulates land-based and online casinos under its licensing authority, ensuring AML/CTF/CPF supervision and compliance of gaming operators within its jurisdiction.

- The **Cagayan Economic Zone Authority (CEZA)** exercises supervisory and regulatory functions over gaming operators licensed within the Cagayan Special Economic Zone & Freeport, including AML/CTF/CPF oversight of gaming-related DNFBPs under its authority.

- The **Aurora Pacific Economic Zone and Freeport Authority (APECO)** regulates enterprises operating within its economic zone, including gaming entities and other covered persons, and is responsible for enforcing AML/CTF/CPF compliance obligations within its jurisdiction.

- Specialized bodies under the NACC address TF and PF, including the **PF Sub-Committee (PFSC)**.

- Law Enforcement and other government agencies under the sub-committees of the **NACC**.

II. Methodology

ML and TF Methodology

The NRA applies the **World Bank National ML/TF Risk Assessment Toolkit**, which defines risk as a function of **threat** and **vulnerability**:

- **Threat:** The scale, nature, and dynamics of predicate crimes that generate illicit proceeds requiring laundering, or the sources of TF funds.
- **Vulnerability:** The characteristics of the national system—laws, institutions, sectors, products, and infrastructure—that may be exploited for ML/TF.

The toolkit includes:

- **National Threat Module:** Assesses threats across major predicate crimes.
- **National Vulnerability Module:** Evaluates the country's overall AML/CTF capacity and systemic safeguards.
- **Sectoral Vulnerability Modules:** Cover banking, securities, insurance, and other financial and DNFBP sectors.

For sectoral assessments, working groups applied the standard World Bank structure:

- **General AML Controls:** Supervision, sanctions, CDD framework, STR reporting, and beneficial ownership (BO) information.
- **Inherent Vulnerability Factors:** Product features, client base, cash intensity, cross-border exposure, and complexity.
- **Product-Specific Controls:** Enhanced CDD for higher-risk products where applicable.

The assessment period (**2021–2024**) was selected to capture post-Second NRA trends, validate improvements post FATF greylisting, and align with the preparation for the next APG Mutual Evaluation.

PF Methodology

PF risk was assessed using a dedicated approach aligned with **FATF Recommendation 1**, in relation to **Recommendation 7**, its Interpretive Note, and relevant **UN Security Council Resolutions**, particularly those concerning the DPRK and Iran.

The PF NRA considered:

- **Threat:** Trade, financial, or other channels that could be misused to finance WMD-related programs.
- **Vulnerability:** The strength and implementation of TFS, export controls, and awareness among authorities and private sector actors.
- **Consequence:** Potential impact on national security, foreign policy, and the financial system.

Data collection combined specialized questionnaires for government agencies and private sector stakeholders with legal and institutional analysis.

Virtual assets and VASPs

Recognizing emerging risks from **virtual assets (VAs)** and **virtual asset service providers (VASPs)**, the NRA incorporated the **World Bank VA/VASP Risk Assessment Guidance** and **FATF standards**, which require jurisdictions to identify and mitigate ML/TF risks associated with VA ecosystems.

Risk Rating Scale

Risk, threat, and vulnerability were expressed using **qualitative bands**, supported by numerical scores in internal working documents:

- **Low**
- **Medium-Low**
- **Medium**
- **Medium-High**
- **High**

In this public version, numerical scores (0.00 to 1.00) are used interchangeably with qualitative bands.

IV. National Money Laundering Risk

The overall **Money Laundering (ML) risk** for the Philippines is assessed as **Medium–High** for the period **2021–2024**. This reflects the combined effect of a **High national ML threat level** and a **Medium national ML vulnerability level**, resulting in a risk environment where the scale of illicit proceeds remains substantial and system-wide controls—though strengthened—are not yet sufficient to fully counter prevailing threats.

Threats

The NRA confirms that a relatively small number of **predicate crimes account for the bulk of ML risk** in the Philippines. Threat ratings consider:

- Estimated value of illicit proceeds
- Frequency of related STRs and cases
- Typology complexity
- Cross-border impact

High-Threat Predicate Crimes

- **Illegal Drug Trafficking:**

Remains one of the largest sources of illicit proceeds. Methamphetamine ("shabu") dominates in value, with marijuana significant by volume. Major seizures, parallel financial investigations, and STR patterns indicate laundering through banks, MSBs, pawnshops, front companies, casinos, and real estate.

- **Fraud and Swindling (including cyber fraud and online investment scams):** Generates substantial dispersed proceeds, often involving large numbers of victims and sophisticated online schemes. Banks and EMI-NBFIs report rising STRs linked to suspected fraud and account takeovers.

- **Environmental Crimes:**
  Illegal logging, wildlife trafficking, illegal mining, and related activities produce high-value proceeds, often commingled with legitimate trade flows and laundered via cash-intensive businesses and trade-based schemes.

- **Tax Crimes:**
  Newly and explicitly covered as predicate offenses under AMLA amendments. Estimated revenue leakage is significant, with typologies involving under-declaration of income, false invoicing, and complex schemes using corporations, professionals, and cross-border trade.

Medium-High Threats

- **Corruption and Bribery:**
  Includes high-level and systemic corruption, which continues to pose serious ML threats despite some progress in enforcement and preventive measures.

- **Securities Fraud and Investment Scams:**
  Large-scale unregistered investments and market abuse schemes generate significant proceeds, often channeled through banking and securities sectors.

- **Online Sexual Abuse and Exploitation of Children (OSAEC):**
  A growing digital crime area with international dimensions, involving relatively small individual transactions but substantial cumulative proceeds.

- **Kidnapping for Ransom and Related Extortion:**
  Increasingly sophisticated, with occasional use of virtual assets and casino channels for layering.

Medium threats

Smuggling, human trafficking, intellectual property violations, and certain forms of organized theft remain significant but generally smaller in scale compared to the high-threat categories. Nonetheless, these crimes present important typologies (e.g. cash couriers, trade mis-invoicing, and front companies) that also feature in other predicate areas.

Cross-border patterns

Cross-border ML risks arise mainly from:

- Payments to foreign suppliers and accomplices in the drug trade;
- online fraud/scams involving victims abroad (including diaspora-linked corridors);
- Use of offshore accounts, shell companies, and foreign casinos;
- Flows into and out of the Philippines via remittance channels and, to a lesser extent, virtual assets;
- International bank wire transfers, including correspondent banking and inter-bank settlement channels used to move value across borders and support layering through overseas counterparties; and
- Trade-based payments and trade finance (TBML) linked to import/export activity, including the use of commercial invoicing and trading structures to transfer value across jurisdictions.

The international FIU survey (33 respondent FIUs) indicates that:

- Most jurisdictions have observed few or no ML/TF cases linked to the Philippines;
- None rated the Philippines as a high ML/TF threat, and only a small number gave a medium rating;
- Where activity is observed, it tends to be concentrated in specific cases involving fraud, drug trafficking proceeds, or online gambling; and
- On TF, most FIUs reported no or very limited cases involving Philippine links.

This combined evidence base supports a **Medium-High** overall cross-border ML risk rating: the **FIU survey** suggests limited international visibility and generally low prioritization, while **domestic STR and case analysis** indicate a **high cross-border threat signal** that is nonetheless concentrated in repeat typologies and specific regional corridors rather than being broad-based across the system. The Medium-High rating, therefore, reflects a high threat, moderated by a **medium vulnerability**, reinforcing the need for sustained cross-border transaction monitoring and prioritized operational cooperation with key counterpart FIUs.

National Vulnerability

National ML vulnerability is assessed as **Medium**, with a vulnerability score of **0.51 on a 0–1 scale**. This reflects a balanced assessment of strengthened systemic controls and remaining structural weaknesses. In parallel, **national ML combating ability** improved to **0.67 (Medium-High)** from **0.60 of the 2nd NRA**, indicating a more robust legal, institutional, and operational response, though important gaps persist.

At the sectoral level, the **post-control ML vulnerability index** is around **0.68 (Medium–High)**, with some sectors significantly more exposed than others.

Strengths

- A significantly strengthened legal and regulatory framework (expanded coverage and predicate offenses, PF treated as a predicate to ML/subjects to TFS obligations, reinforced CDD, including beneficial ownership verification requirements);
- More effective FIU, law enforcement, and prosecutorial structures, including increased use of financial intelligence in investigations and asset recovery;
- Improved supervision across many sectors, especially banks and other BSP-supervised institutions, supported by risk-based frameworks and the use of corrective measures; and
- Enhanced cross-border cooperation and use of international platforms, enabling more timely exchange of information on ML/TF/PF cases and typologies.

These elements underpin the improvement in ML combating ability and have helped moderate overall vulnerability despite high and persistent threats.

Persistent Vulnerabilities

- A large informal and cash-driven economy creates opaque channels for placement and movement of illicit funds outside the fully supervised system;
- Inconsistent STR coverage and quality across sectors limits the analytical value of financial intelligence, particularly among newer or smaller reporting entities;
- Beneficial ownership transparency and verification gaps persist, including constraints on timeliness, completeness, and verification, and limited direct usability of BO data by covered persons for real-time CDD validation;
- Emerging and high-velocity channels (digital payments/e-money, online onboarding models, and virtual assets) carry elevated inherent risks and—in some segments—controls and monitoring capabilities remain in a maturation phase, particularly for transaction monitoring effectiveness and internal compliance tooling; and
- Varying AML/CTF/CPF capacity among DNFBPs, small financial institutions, and geographically dispersed service providers results in uneven implementation and slows consistent risk-based compliance across the system.

The persistence of these vulnerabilities indicates that, while foundational reforms have been effective, **system resilience remains uneven across sectors and regions**. The Medium–High sectoral vulnerability rating reflects this pattern: banks and core financial institutions benefit from mature controls, whereas **casinos, real estate, MSBs, pawnshops with remittance services, and VASPs exhibit higher residual vulnerabilities**.

Cross-cutting issues—such as integrity risks, resource constraints in some agencies, and data gaps (particularly for certain predicate crimes and DNFBP sub-sectors)—also influence the national vulnerability profile and must be addressed to further strengthen ML combating ability in the updated national strategy.

Medium–High Overall ML Risk

Integrating national threat and vulnerability assessments yields an **overall ML risk rating of Medium–High**, signifying a risk environment where:

- The volume and complexity of illicit proceeds remain substantial, driven by entrenched, high-revenue predicate crimes;
- National controls, while institutional controls improved, key gaps remain (e.g., beneficial ownership transparency, law enforcement capacity, and oversight of informal/technology-driven channels);
- Criminal networks continue to adapt rapidly, exploiting both traditional channels (cash, remittance networks, real estate) and emerging technologies (e-money, VASPs, digital platforms);
- Sectoral vulnerabilities are uneven, with casinos, real estate, MSBs, pawnshops with remittance services, and VASPs showing greater susceptibility to misuse;
- Cross-agency coordination and data integration, though enhanced through reforms supporting FATF delisting / grey list exit, require continued institutionalization for long-term sustainability.

The **Medium–High rating** reflects a risk environment that is significant but manageable, provided reforms remain sustained and targeted—particularly in high-impact and high-volume sectors.

Implications for Policy and Supervision

The assessment highlights several implications:

- Sustained, risk-based supervision and credible enforcement are critical in higher-risk financial and DNFBP sectors and geographic hotspots, to close compliance gaps exploited for layering and integration.
- Beneficial ownership transparency must continue to improve by strengthening the timeliness, accessibility, and verification of BO information, and progressing toward a more centralized BO mechanism accessible to competent authorities.
- Digital-era risks require accelerated modernization of controls, especially in EMI-NBFIs, OPS, and VASPs, including stronger analytics/monitoring and continued implementation of relevant standards (e.g., Travel Rule-related controls for VASPs).
- Parallel financial investigations and asset recovery should be institutionalized for high-threat predicate crime cases, ensuring early asset tracing and financial intelligence actions through SOPs and coordinated multi-agency case handling.
- Feedback loops with covered persons should be strengthened through typology/red-flag advisories and structured feedback on STRs to improve STR quality and frontline detection.

These assessment highlights will feed into the development of the National AML/CTF/CPF Strategy (NACS) 2026–2030 and related action plans, helping ensure that priorities, resources,

and supervisory focus are aligned with the highest-risk threats, sectors, and channels identified in the NRA.

V. Sectoral ML Vulnerabilities (Qualitative Overview)

The NRA assessed sectoral vulnerabilities post-controls using a common framework. Scores were converted into qualitative bands; the summaries below reflect these bands rather than numeric values.

Banking Sector – Medium Vulnerability

Banks hold the largest share of financial system assets and handle most formal financial flows. Inherent ML/TF/PF risk is **high** due to:

- Broad product and service offerings;
- High transaction volumes;
- Extensive branch and digital networks.

Banks are exposed to proceeds from **drug trafficking, fraud, cybercrime, OSAEC, trafficking in persons, environmental crime, and tax crimes**.

Post-control vulnerability: Medium, supported by:

- A robust AML/CTF/CPF legal and regulatory framework;
- Risk-based supervisory tools (e.g., Supervisory Assessment Framework, ML/TF/PF Risk Assessment System);
- Strengthened institutional controls, compliance culture, and board-level oversight; and
- Regular examinations, thematic reviews, and active enforcement by BSP and AMLC.

Residual vulnerabilities: Effectiveness of transaction monitoring, alert management, ongoing CDD for higher-risk customers and digital channels, and STR quality/timeliness.

Money Service Businesses (MSBs) – Medium-High Vulnerability

MSBs (Stand-alone Remittance Transfer Companies and Money Changers/Foreign Exchange Dealers) are inherently vulnerable due to:

- Cash-intensive operations;
- Wide geographic reach; and
- Cross-border transfers.

They often serve as entry points for migrant and rural clients into the formal financial system but can facilitate placement and layering if abused.

Overall vulnerability: Medium-High, reflecting:

- Medium-High inherent vulnerability; and

- Medium quality of AML/CTF/CPF controls.

Key mitigants:

- Structured registration and licensing regime, including network registration and fit-and-proper requirements;
- Risk-based supervision and thematic reviews;
- Active enforcement, including cancellations and disqualification of illegal operators; and
- Coordination with local government units to detect and sanction unregistered MSBs.

Persistent risks: Prevalence of cash, smaller operators with limited compliance capacity, and challenges in identifying informal or unregistered operators.

Pawnshops (Stand-alone Pawnshops and Pawnshops with Corollary MSB Services) – Medium Vulnerability

Pawnshops play a major role in financial inclusion. Traditional pawning transactions are generally low risk, but remittance and FX services increase exposure to ML/TF risks.

Overall vulnerability: Medium, driven by:

- Medium inherent vulnerability (higher where remittance services are offered);
- Medium quality of AML/CTPF controls, including risk-based supervision, licensing, and enforcement.

Key mitigants:

- Enhanced supervisory approach (including RAMPS) and proactive measures against unregistered/unauthorized operators; and
- A broad range of proportionate enforcement tools (directives, restrictions, penalties, revocations, disqualifications).

Residual vulnerabilities: Effectiveness of suspicious activity reporting and further strengthening of compliance systems in smaller networks.

Electronic Money Issuers – Non-Bank FIs (EMI-NBFIs) – Medium Vulnerability

EMI-NBFIs are central to the digital payments ecosystem. Inherent vulnerability is Medium-High due to:

- Rapid growth in e-wallet usage;
- High volumes of small-value transactions;
- Reliance on agents and cash-in/cash-out points; and
- Exposure to fraud, mule accounts, and online scams.

Post-control vulnerability: Medium, supported by:

- A robust legal framework and clear AML/CTF/CPF obligations;
- BSP's entry controls and risk-based supervision; and
- Enforcement of administrative and criminal sanctions.

Areas for improvement: Transaction monitoring for digital typologies, risk-based CDD for higher-risk use cases, compliance staffing and training, and PF awareness.

Non-Stock Savings and Loan Associations (NSSLAs) – Medium-Low Vulnerability

NSSLAs are closed-membership, non-stock, non-profit institutions that provide basic savings and loan products exclusively to members of a well-defined group (WDG).

Inherent vulnerability is Low due to:

- a limited and simple product suite (primarily deposits/capital contributions and member loans);
- a restricted customer base (WDG members) and generally domestic transaction profile; and
- a more contained operating model, with lower exposure to complex products and high-risk channels.

Post-control vulnerability: Medium-Low, reflecting low inherent exposure moderated upward by:

- dealings with politically exposed persons (PEPs) in certain cases; and
- Medium AML/CTPF controls, supported by BSP supervision and enforcement, but with remaining compliance gaps.

Areas for improvement: strengthen PEP-related controls and the effectiveness of the compliance function, and improve the timeliness and quality of CT/ST reporting.

Trust Entities NBFIs– Medium Vulnerability

NBFIs with trust licenses play a material role in the financial system, with assets under management equivalent to about 11% of total banking system assets and a client base of around 2.4 million.

Inherent vulnerability is **Medium** due to:

- Material scale of fiduciary activities and broad client reach;
- Access to offshore assets through select products/services; and
- Use of agents and non-face-to-face onboarding for select services.

Post-control vulnerability: **Medium**, supported by:

- Medium-High AML/CTPF controls, reflecting comprehensive legal frameworks; and

- Effective AML/CTPF supervision and oversight of TE-NBFIs.

Areas for improvement: Strengthen controls for effective monitoring and reporting of suspicious activities, including enhanced customer risk assessment and sanctions screening—especially for offshore-linked exposures and non-face-to-face onboarding use cases.

Operators of Payment Systems (OPS) – Low to Medium Vulnerability

OPS supports the country's payments infrastructure, and inherent vulnerability varies by business model and exposure to merchant payments and cash interfaces.

Inherent vulnerability ranges from **Low to Medium** due to:

- **Low risk:** Financial Market Infrastructure Operators, network payment processors, affiliate switch networks, payment gateways, and bill payment providers (institutional clients, controlled infrastructures);
- **Medium-Low risk:** Cash-in service providers and clearing switch operators; and
- **Medium risk:** Merchant acquirers and independent ATM deployers [IADS] (high transaction volumes, merchant heterogeneity).

Post-control vulnerability: Low to Medium, supported by:

- BSP regulatory oversight under the NPSA/NCBA (including registration and, where applicable, designation of payment systems);
- Governance requirements and key regulatory issuances (including the merchant payment acceptance framework); and
- Ongoing market surveillance and monitoring.

Areas for improvement: Maintain targeted supervisory focus on higher-exposure OPS (e.g., merchant acquiring, IADs, cash-in services) and continuously strengthen monitoring and risk-indicator reporting as payment typologies evolve.

Securities Sector – Medium Vulnerability

Securities activity can facilitate layering/integration through investment accounts and securities transactions.

Inherent vulnerability: **Medium-High** due to:

- Significant market size and transaction values/volumes, which increase opportunities to camouflage illicit activity;
- Product complexity/diversity and liquidity features (e.g., equities and collective investments), which can obscure transactional patterns and enable rapid movement of value; and
- Diverse client base, including institutional and foreign investors and PEP exposure, with some cross-border investment links (even if not common).

Post-control vulnerability: **Medium**, supported by Medium-High AML controls, including:

- Medium-High quality of operations in securities firms, including suspicious activity monitoring/reporting and a medium-high CDD framework rating;
- Medium-High internal AML policies/procedures, supported by management commitment, compliance function effectiveness, and a comprehensive AML legal framework; and
- SEC-led supervision and examinations, including checks on reporting systems and AMLC registration, complemented by outreach and capacity-building efforts to improve reporting compliance.

Areas for improvement: Strengthen risk-based transaction monitoring (particularly among smaller intermediaries), improve STR quality/supporting documentation, and continue enhancing customer and beneficial ownership identification to support more targeted detection and reporting.

Insurance Sector - Medium-Low Vulnerability

Insurance generally involves slower fund movement and structured pay-outs, reducing attractiveness for rapid laundering, but specific products and channels still require targeted safeguards.

Inherent vulnerability: **Medium-Low** due to:

- Cash value / investment-linked life products (e.g., VUL and single-premium structures) and features such as policy loans and early surrender that can convert value back to cash or near-cash;
- High-value premium payments, including potential misuse of overpayments/refunds and third-party premium arrangements, which can complicate ownership/beneficiary tracing;
- Reliance on a broad agent/broker distribution network, creating exposure to uneven CDD and monitoring and (in some segments) data gaps due to limited survey participation/coverage of intermediaries; and
- Cross-border elements (notably reinsurance/premium flows) that may increase complexity and reduce transaction visibility in specific cases.

Post-control vulnerability: **Medium-Low,** supported by**:**

- A strong AML legal/regulatory base for the sector (AMLA and IC issuances), with "Comprehensiveness of AML Legal Framework" assessed Very High in the NRA inputs referenced in the sector write-up;
- Licensing/fit-and-proper entry controls and risk-based supervision by the Insurance Commission (dedicated AML supervision function, on-site examinations, and thematic reviews, including on TFS); and
- Established compliance arrangements and reporting: compliance units (including monitoring flags for early surrender / multiple cash premium payments) and ongoing CTR/STR reporting to AMLC (with rising STR volumes across the period).

Areas for improvement: Strengthen institutional risk assessment (IRA) uptake and deepen risk-based monitoring and STR quality/consistency, particularly for investment-linked/cash-value products and intermediary channels (agents/brokers and relevant cross-border/reinsurance activity).

Virtual Assets and VASPs – Medium-High Vulnerability

Virtual Assets and VASPs – Medium-High Vulnerability; Controls Evolving

Inherent vulnerability is **High** due to:

- The anonymity and speed of VA transfers, including exposure to DeFi platforms, 24/7 availability, peer-to-peer transactions, transfers to/from unhosted wallets, and use of anonymity-enhancing features that enable rapid settlement;
- Heavy reliance on technology-aided/digital onboarding (predominantly via mobile applications), which increases customer identification/verification and monitoring challenges at scale;
- Recurring typologies linked to investment scams, cybercrimes, and kidnap-for-ransom, with STR-based typologies also highlighting the use of VAs/VASPs in online sexual exploitation and frauds/scams; and
- Spillover exposure from unlicensed/unregistered VASPs identified through surveillance (including entities not licensed in the Philippines or elsewhere).

Post-control vulnerability: **Medium-High**, supported by:

- A comprehensive, activity-based legal and regulatory framework for core VASP activities under BSP authorities (with complementary SEC coverage for VA-related offering/sale activities);
- Medium-High mitigating measures anchored on the comprehensiveness of the AML/CFT legal framework, entry controls, and supervision/monitoring mechanisms (rated high for several government-level measures); and
- Strengthening VASP internal controls, including use of blockchain analytics/sanctions screening tools and travel-rule technology solutions, while noting interoperability issues that still affect effective information sharing.

Areas for improvement: Strengthen the effectiveness of VASP compliance and internal controls—particularly transaction monitoring/alert management for key typologies, TFS implementation, and travel-rule interoperability—and reinforce counterparty due diligence to limit exposure to unlicensed VASPs and high-risk wallet/exchange relationships.

DNFBPs – Casinos, Real Estate, and Other Professions

Within DNFBPs:

Casinos and Gaming - Medium-High

Inherent vulnerability is **High due** to**:**

- cash-intensive operations;
- high-value transactions; and
- the potential for rapid conversion of cash to chips and back (including junket/VIP activity).

Post-control vulnerability remains **Medium-High**, supported by:

- strengthened AML obligations since casinos' coverage under AMLA (RA 10927);
- improved CDD and reporting (CTRs/STRs);
- probity/fit-and-proper controls; and
- more structured supervisory engagement by PAGCOR/AMLC.

Areas for improvement: ensure more consistent implementation across casino types/operators, strengthen transparency and uniform application of fit-and-proper/junket controls, and sustain effective monitoring of high-cash and cross-border risk exposures.

Real Estate Developers and Brokers - Medium-High

Inherent vulnerability is **High**, due to:

- high-value transactions;
- exposure to cash payments;
- risks of over/under-pricing; and
- the use of complex structures or proxies that can obscure beneficial ownership.

Post-control vulnerability is **Medium-High, supported by:**

- sector's coverage under AMLA (via RA 11521); and
- AMLC registration and risk-based supervision tools (including DNFBP risk rating and examination programs), but controls are still being embedded across a large and fragmented population, with reporting and compliance capacity uneven.

Areas for improvement: strengthen beneficial ownership verification and documentation for higher-risk transactions, improve STR quality and timeliness, expand AML awareness through professional and sector touchpoints, and sustain supervisory coverage given the sector's scale.

Other DNFBPs - Medium to Medium-Low

Vulnerabilities are **uneven** across professions and high-value goods dealers.

Lawyers, accountants, and company service providers are assessed **Medium** overall, reflecting gatekeeper exposure (e.g., facilitating transactions or structures that may obscure ownership) alongside still-maturing and variable compliance uptake.

Dealers in precious metals and stones are **Medium** overall (with relatively higher inherent vulnerability), reflecting portability and high-value dealing risks moderated by AML coverage and controls;

Car dealers are **Medium-Low** overall, reflecting comparatively more identifiable assets but continuing exposure where cash purchases or nominee buyers are used.

Areas for improvement across these DNFBPs: strengthen AML awareness and compliance functions, improve consistency of CDD/recordkeeping, and raise the effectiveness and timeliness of STR reporting to reduce under-detection.

Financial Inclusion Products - Low to Medium Net ML Risk

Financial inclusion products provide simplified, low-cost entry points into the formal financial system.

Inherent vulnerability is generally **Low,** but rises to **Medium** for transfer-enabled products, due to:

- Continuing low-value transactions and well-defined product features for MF loans, BDAs, microinsurance, and pawning;
- Higher exposure to predicate-crime typologies reflected in STRs for pawnshop remittance services and basic e-money wallets; and
- Broader access and reach (including via agents and transfer touchpoints) that can be exploited for faster movement of funds in higher-risk use cases.

Net ML risk: Low for MF loans, BDAs, microinsurance, and pawning; and **Medium** for pawnshop remittance services and e-money basic wallets.

Risk is moderated by:

- Tiered/risk-based CDD, including KYC/verification using government-issued IDs (with the National ID emphasized) and alternative documents where applicable (e.g., for BDAs); and
- Product-level limits and eligibility constraints (e.g., small-value thresholds/maximum balance limits for BDAs; and transaction ceilings plus restrictions such as no cross-border transactions for microinsurance).

Areas for improvement: Strengthen monitoring and STR reporting for fraud and **money-mule typologies** affecting e-money and remittance channels and sustain risk-based oversight of agent/transfer touchpoints where higher-risk activity concentrates.

VI. Terrorism Financing Risk

The NRA assesses overall TF risk as **Medium**, comprising:

- **TF Threat:** Medium
- **TF Vulnerability:** Medium-Low

Compared with the previous cycle, TF risk has moderated due to:

- Sustained security operations weakening domestic terrorist groups;
- A relatively low number of confirmed TF cases;
- Strengthened TF legal and institutional frameworks (TFPSA, Anti-Terrorism Act, and related regulations).

Residual risk remains significant because even small-value funding can enable terrorist activity.

Main Characteristics

- **Geographic hotspots:** Concentrated in selected provinces in Mindanao, where remnants of local terrorist groups and affiliates operate. (Public version refers only to regions, not specific localities.)
- **Funding methods:** Small cash donations, local fundraising, family/community networks, remittances, cash couriers, and occasional abuse of NPOs and informal value transfer systems.
- **Cross-border exposure:** Some links identified between domestic groups and foreign supporters, including cross-border transfers and facilitation. International cooperation remains critical.

Mitigation Measures

- Designation and freezing mechanisms under TFPSA and UN-related resolutions;
- Enhanced coordination among security forces, FIU, prosecutors, and supervisors;
- Risk-based oversight of NPOs to prevent misuse while preserving legitimate activities;
- Integration of TF risk indicators into STR reporting guidance and training; and
- Systematic use of financial intelligence in terrorism investigations and prosecutions.

Residual risks: Adaptability of terrorist networks, potential use of new technologies (including VAs) for TF, and the need for sustained vigilance in areas where overt terrorist activity has declined but enabling networks persist.

VII. Proliferation Financing Risk

The first PF National Risk Assessment rates national PF risk as **Medium**, characterized by:

- **Low inherent external threat:** Limited links to PF high-risk jurisdictions;
- **Moderate (Medium-High) vulnerabilities:** Legal, institutional, and private sector frameworks; and
- **Potentially high consequence:** Significant implications for national security and foreign policy if PF abuse occurs.

Threat

The Philippines has limited trade, financial, and political exposure to jurisdictions subject to extensive PF-related sanctions (e.g., DPRK and Iran). Most trade is with partners aligned with the international non-proliferation regime. No confirmed PF cases have been reported to date.

Vulnerabilities

Structural vulnerabilities include:

- Fragmented responsibilities and varying expertise across agencies handling export controls, customs, trade, and AML/CFT;
- Limited PF-specific awareness and internal controls among trade-related companies, logistics providers, customs brokers, and other non-financial actors; and
- Need to integrate PF concerns into AML/CTF risk assessments and compliance programs across financial institutions and DNFBPs.

Survey results indicate that many agencies and private sector respondents lack dedicated PF risk policies or assessments, underscoring the need for targeted guidance and capacity building.

Legal and Institutional Progress

Since 2021, key reforms include:

- AMLA amendments (RA 11521) establishing TFS for PF and empowering AMLC to freeze assets linked to UN-designated proliferators;
- Creation of the PF Sub-Committee (PFSC) under NACC for policy coordination;
- Issuance of guidance by BSP and other regulators to incorporate PF into sanctions screening and risk management; and
- Ongoing development of a comprehensive CPF legal and institutional framework, including clearer procedures for listing, delisting, and unfreezing.

Priority PF Actions

- Enact a comprehensive CPF law consolidating and clarifying PF obligations;
- Clarify roles and communication channels among AMLC, STMO, customs, foreign affairs, defense, and intelligence agencies;
- Strengthen awareness and controls among trade and logistics actors through targeted training and outreach;
- Integrate PF risk into AML/CTF risk assessments, CDD, and sanctions screening for financial institutions and DNFBPs; and
- Enhance international cooperation with like-minded countries on export control and PF risk intelligence.

VIII. Priority Actions and Link to National Strategies

The NRA's findings directly inform the **National AML/CTF/CPF Strategy (2026–2030)** and sectoral action plans. Priority actions are grouped as follows:

Legal and Policy Reforms

- Consolidate PF obligations into a comprehensive **Counter-Proliferation Financing (CPF) law**;
- Further strengthen **beneficial ownership transparency** for legal persons and arrangements, ensuring data quality and timely access for competent authorities; and
- Review and refine **TF provisions and implementation** to maintain alignment with evolving risks and international standards.

Supervisory and Regulatory Strengthening

- Deepen **risk-based supervision** of higher-risk sectors, particularly casinos, real estate, MSBs, pawnshops with remittance services, and VASPs;
- Continue enhancing AML/CTF/CPF frameworks for **EMI-NBFIs, OPS, and other digital providers**, ensuring proportionate but effective controls; and
- Strengthen **sector-specific guidance** on ML/TF/PF typologies, STR red flags, and sanctions compliance, including for DNFBPs.

Law Enforcement and FIU Capacity

- Expand capacity for **parallel financial investigations** across major predicate crimes—especially drugs, fraud, environmental crimes, tax crimes, and corruption;
- Enhance **asset tracing, freezing, and forfeiture capabilities**, including non-conviction-based mechanisms where permitted; and
- Use **FIU intelligence more systematically** to support investigations and prosecutions, including for TF and PF.

Private Sector Compliance and Awareness

- Promote robust, **risk-based enterprise-wide risk assessments** across banks, EMI-NBFIs, MSBs, casinos, real estate, VASPs, and other covered entities;
- Improve training and internal controls on **emerging risks** (digital payments, VAs, cyber fraud, PF) and handling higher-risk customers and transactions; and
- Encourage **industry-level cooperation and information sharing** (e.g., typology exchanges, common red flags) within data protection boundaries.

Data, Analytics, and Technology

- Upgrade **STR analytics and data integration** across AMLC, supervisors, and law enforcement agencies;

- Improve **data collection on predicate crimes**, especially where gaps exist (e.g., environmental crimes, PF-related exposures); and
- Leverage **advanced analytics and network analysis tools** to identify complex ML/TF/PF patterns across sectors.

These priorities will be reflected in the updated **National AML/CTF/CPF Strategy (2026-2030)** and agency-level implementation plans. Progress will be tracked through measurable outputs and outcomes, including:

- Increased use of financial intelligence;
- Improved asset recovery;
- More risk-based supervision; and
- Sustained compliance with international standards.

Annexes

Annex 1- Glossary of Acronyms and Key Terms

AML – Anti-Money Laundering.
AMLA – Anti-Money Laundering Act of 2001, as amended (including RA 11521), which sets out the Philippines' core AML/CTF/CPF obligations, predicate offenses, reporting requirements, and targeted financial sanctions framework.
AMLC – Anti-Money Laundering Council, the Philippines' Financial Intelligence Unit (FIU) and primary AML supervisor for non-prudentially regulated sectors.
AML/CTF/CPF – Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing – the overarching framework used in this NRA for addressing ML, TF, and PF risks.
ASN – Affiliate Switch Network – a type of operator of payment systems that provides network switching services between affiliated institutions.
ATMs – Automated Teller Machines – electronic terminals that provide cash withdrawal and related services; some are operated by independent ATM deployers classified under OPS.
BIR – Bureau of Internal Revenue, the primary tax authority; referenced in underlying sectoral work on tax crimes.
BO – Beneficial Ownership / Beneficial Owner – the natural person(s) who ultimately owns or controls a customer or on whose behalf a transaction is being conducted.
BOC – Bureau of Customs, a key border-control and trade-related authority relevant for ML/TF/PF and PF implementation.
BSP – Bangko Sentral ng Pilipinas, the central bank of the Philippines and prudential/AML supervisor of banks, MSBs, EMI-NBFIs, OPS, and selected trust entities.
CDD – Customer Due Diligence – the set of identification, verification, and ongoing monitoring measures that covered persons must apply to their customers and beneficial owners.
CEZA – Cagayan Economic Zone Authority, which exercises supervisory and regulatory functions over gaming operators and other covered entities licensed within the Cagayan Special Economic Zone & Freeport.
CPF – Counter-Proliferation Financing – measures to prevent, detect, and disrupt the provision of funds or financial services used for the proliferation of weapons of mass destruction.
CSPs – Company Service Providers – professionals or firms that provide company formation, management, registered office, or related services and are treated as DNFBPs when engaged in covered activities.
CTR / CTRs – Covered Transaction Report(s) – reports filed with the AMLC for transactions that meet prescribed value thresholds under the AMLA.
DeFi – Decentralized Finance
DNFBP / DNFBPs – Designated Non-Financial Businesses and Professions, including casinos, real estate developers and brokers, dealers in precious metals and stones, lawyers and accountants engaged in covered activities, and company service providers.
DPRK – Democratic People's Republic of Korea – a jurisdiction subject to extensive UN sanctions, referenced in the PF NRA as an example of a PF-high-risk jurisdiction.
EMI-NBFIs / EMINBFIs – Electronic Money Issuers – Non-Bank Financial Institutions, non-bank entities licensed to issue e-money and operate wallets and digital payment platforms.
FATF – Financial Action Task Force, the global standard-setter for AML/CTF/CPF; it placed the Philippines under increased monitoring ("grey list") and removed it from the list in February 2025.

FIU / FIUs – Financial Intelligence Unit(s). In the Philippines, the FIU is the AMLC; foreign FIUs participate in information exchange and in the international survey cited in the NRA.
FMI / FMIs – Financial Market Infrastructure(s) – systemically important payment, clearing, or settlement systems categorized as a type of OPS with generally low inherent ML/TF/PF risk.
GDP – Gross Domestic Product – the total value of goods and services produced in the Philippines; used to provide macroeconomic context to the NRA.
IADS - Independent ATM deployers.
IC – Insurance Commission – the supervisor of life and non-life insurers, pre-need companies, and related intermediaries, including for AML/CTF/CPF purposes.
MF - Microfinance
ML – Money Laundering – the processing of criminal proceeds to disguise their illegal origin so they appear to come from legitimate sources.
ML/TF – Money Laundering and Terrorism Financing – used jointly when describing combined risk assessments, controls, or typologies.
ML/TF/PF – Money Laundering, Terrorism Financing, and Proliferation Financing – shorthand for the three categories of financial crime risk assessed in this NRA.
MSB / MSBs – Money Service Business(es) – stand-alone remittance companies and money changers/FX dealers offering remittance and foreign exchange services.
NACC – National AML/CTF/CPF Coordinating Committee, the high-level inter-agency body that provides overall policy direction and coordination for AML/CTF/CPF.
NACS – National AML/CTF/CPF Strategy, the multi-year national strategy and action plan informed by the findings of this NRA.
NBI – National Bureau of Investigation – a key law enforcement authority involved in investigation and prosecution of ML, TF, and predicate crimes.
NCBA – New Central Bank Act (R.A. No. 7653, as amended).
NPO / NPOs – Non-Profit Organization(s), including foundations and non-stock, non-profit entities that may be vulnerable to abuse for TF or PF but also play vital legitimate roles.
NPSA – National Payment System Act (R.A. No. 11127).
NRA – National Risk Assessment – the structured national-level assessment of ML, TF, and PF risks; this document is the Third NRA for the Philippines.
NSSLA / NSSLAs – Non-Stock Savings and Loan Association(s), closed-membership institutions providing basic savings and credit services to defined groups, assessed as having medium-low ML vulnerability.
OFW / OFWs – Overseas Filipino Worker(s), whose remittances are a significant source of foreign exchange and a key factor in the structure of the remittance and MSB sectors.
OPS – Operators of Payment Systems – entities that maintain or operate payment systems or provide payment services (including FMIs, network payment processors, merchant acquirers, payment gateways, bill-payment providers, cash-in service providers, and clearing switch operators).
OSAEC – Online Sexual Abuse and Exploitation of Children – a growing digital predicate crime involving cross-border financial flows and online platforms.
PAGCOR – Philippine Amusement and Gaming Corporation, the regulator and AML supervisor of casinos and other gaming operations within its licensing authority.
PEP / PEPs – Politically Exposed Person(s) – individuals who are or have been entrusted with prominent public functions (and their close associates), requiring enhanced due diligence due to higher corruption and ML risk.

PF – Proliferation Financing – the provision or collection of funds, financial assets, or services used to finance the proliferation of weapons of mass destruction, as defined in international standards and domestic law.
PF NRA – Proliferation Financing National Risk Assessment – the Philippines' first dedicated assessment of PF risk, integrated into this Third NRA.
PFSC – Proliferation Financing Sub-Committee, a specialized sub-committee under the NACC responsible for coordinating PF policies and implementation.
PNP – Philippine National Police – the main national police service, including units involved in financial crime and terrorism-related investigations.
RA – Republic Act – a law enacted by the Congress of the Philippines; individual acts are cited in the NRA by their RA number (e.g., RA 11521).
RAMPS - Recalibrated Approach to MSBs and Pawnshops Supervisory Assessment Framework.
SAFr - Supervisory Assessment Framework.
SEC – Securities and Exchange Commission – the corporate, capital markets, and certain DNFBP/NPO regulator, including AML/CTF/CPF supervision of covered entities under its authority.
SOP – Standard Operating Procedure.
STMA – Strategic Trade Management Act – the law providing the basis for strategic goods and export controls relevant to counter-proliferation and PF risk mitigation.
STMO – Strategic Trade Management Office – the specialized office under the Department of Trade and Industry responsible for implementing strategic trade controls under the STMA.
STR / STRs – Suspicious Transaction Report(s) – reports submitted by covered persons to the AMLC when a transaction is suspected to be linked to ML, TF, PF, or related predicate crimes, regardless of amount.
TFS – Targeted Financial Sanctions – restrictive measures (such as freezing of funds or assets) applied without delay to designated persons and entities, including those linked to terrorism and proliferation.
TF – Terrorism Financing – the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used, or in the knowledge that they are to be used, in whole or in part, to carry out terrorist acts or support terrorist organizations.
TFPSA – Terrorism Financing Prevention and Suppression Act of 2012, the core law criminalizing TF and establishing preventive and freezing mechanisms, complementing the Anti-Terrorism Act.
UN – United Nations – the primary international organization whose Security Council Resolutions establish binding obligations on member states concerning TF and PF-related sanctions.
VA / VAs – Virtual Asset(s) – a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes (e.g. cryptocurrencies).
VASP / VASPs – Virtual Asset Service Provider(s) – entities that conduct activities such as exchange between virtual assets and fiat currencies, transfer of virtual assets, or safekeeping of virtual assets, and are subject to AML/CTF/CPF obligations.
WMD – Weapons of Mass Destruction – nuclear, chemical, or biological weapons whose proliferation is the focus of PF and CPF measures.

Annex 2 - Risk rating scale

RATING	Numerical Equivalent
Low	0.00-0.20
Medium-Low	0.21-.40
Medium	0.41-0.60
Medium-High	0.61-0.80
High	0.81-1.00

This framework applies a five-level risk rating **(low, medium-low, medium, medium-high, and high)** to enable a risk-based approach in assessing, prioritizing, and managing threats. Each tier determines the level of intervention, control intensity, and resource allocation needed to ensure proportional and effective risk mitigation.

Low Risk

Minimal likelihood and impact. Basic controls and routine monitoring are sufficient. Resources remain limited as the risk does not warrant significant intervention.

Medium-Low Risk

Slight potential for escalation. Existing controls generally work but may need minor adjustments. Regular reviews support early detection of changes.

Medium Risk

Balanced likelihood and impact. Requires ongoing monitoring, moderate preventive measures, and proportionate resource allocation to prevent escalation.

Medium-High Risk

High probability or notable consequences. Controls may be insufficient; enhanced measures and increased oversight are necessary. Additional resources and contingency plans are prioritized.

High Risk

Significant likelihood and severe impact. Demands immediate action, strict controls, continuous supervision, and major resource commitment.

Applying this risk-based approach ensures that controls, attention, and resources are aligned with the level of risk. This will promote proactive management, efficient prioritization, and strengthened resilience.

Annex 3. Participating agencies and sectors

AGENCIES INVOLVED IN THE NATIONAL RISK ASSESSMENT
Anti-Money Laundering Council
Anti-Terrorism Council
Armed Forces of the Philippines
Association of Bank Compliance Officers
Association of Bank Remittance Officers, Inc.
Association of Certified Public Accountants in Public Practice
Association of Remittance Company Compliance Officers
Aurora Pacific Economic and Freeport Zone
Bangko Sentral ng Pilipinas
Bankers Association of the Philippines
Bureau of Customs
Bureau of Immigration
Bureau of Internal Revenue
Cagayan Economic Zone Authority
Capital Markets Integrity Corporation
Caucus of Development NGO Networks
Chamber of Thrift Banks
Confederation of Philippine Jewelers, Inc.
Cooperative Development Authority
Department of Environment and Natural Resources
Department of Finance
Department of Foreign Affairs
Department of Justice
Department of National Defense
Department of Social Welfare and Development
Department of the Interior and Local Government
Department of Trade and Industry
Insurance Commission
Integrated Bar of the Philippines
Intellectual Property Office of the Philippines
Intelligence Service Armed Forces of the Philippines
Inter-Agency Council Against Trafficking
Investment Companies Association of the Philippines
Investment House Association of the Philippines
Land Registration Authority
National Bureau of Investigation
National Development Company
National Intelligence Coordinating Agency
National Privacy Commission
National Security Council
Office of the Ombudsman
Office of the Solicitor General
Palawan Council on Sustainable Development
Philippine Amusement and Gaming Corporation
Philippine Association of Securities Brokers and Dealers, Inc.
Philippine Association of Stock Transfer Agents
Philippine Center on Transnational Crime

Philippine Chamber of Mutual Benefit Associations, Inc.
Philippine Coast Guard
Philippine Council for NGO Certification, Inc.
Philippine Deposit Insurance Commission
Philippine Deposit Insurance Corporation
Philippine Drug Enforcement Agency
Philippine Institute of Certified Public Accountants
Philippine Insurers and Reinsurers Association, Inc.
Philippine Life Insurance Association, Inc.
Philippine National Police
Philippine Ports Authority
Philippine Stock Exchange
Presidential Anti-Organized Crime Commission
Professional Regulation Commission
Rural Bankers Association of the Philippines
Securities and Exchange Commission
Trust Officers Association of the Philippines