EU P2P
Export Control Programme
for Dual-use Goods

CBRN
Centres
of Excellence
An initiative of the European Union

EU AML / CFT
GLOBAL FACILITY

APG
Asia/Pacific Group
on Money Laundering

HANDBOOK OF REGIONAL PROLIFERATION FINANCING RISKS IN SOUTHEAST ASIA

JUNE 2026

Funded by
the European Union

The EU P2P Global Project, the EU AML/CFT Global Facility Project and the Asia/Pacific Group on Money Laundering (APG) organized a regional conference, 7-8 October 2025 in Bangkok, on proliferation finance risks in Southeast Asia[1]. The primary aim of this conference was to encourage and facilitate knowledge exchange and collaboration among Southeast Asian jurisdictions, thus enhancing regional capacities to identify and respond effectively to proliferation finance threats in connection with responses to other illicit finance activities such as money laundering and terrorist financing.

EU P2P Global Project: EU P2P (Partner-to-Partner) Export Control Programme for Dual-use Goods is the European Union's flagship programme for establishing dialogue opportunities with partner countries on the prevention of the proliferation of weapons of mass destruction through the management of international trade and financial transactions.

EU AML/CFT Global Facility: Established in 2017 by the European Commission, the project supports partner countries in strengthening anti-money laundering and counter-terrorism financing measures through technical assistance and capacity building.

Asia/Pacific Group on Money Laundering (APG): An inter-governmental organisation with 41 member jurisdictions dedicated to implementing international standards against money laundering, terrorist financing, and proliferation financing.

EU P2P Export Control Programme for Dual-use Goods

CBRN Centres of Excellence
An initiative of the European Union

EU AML / CFT GLOBAL FACILITY

APG Asia/Pacific Group on Money Laundering

Disclaimer:
This publication was produced with the financial support of the European Union. Its contents are the sole responsibility of the authors and do not necessarily reflect the views of the European Union.

For further information, please contact:

info@global-amlcft.eu
www.global-amlcft.eu

eup2p.dug@expertisefrance.fr

mail@apgml.org
www.apgml.org

© Visual credits: Images licensed from Envato. Icons licensed from Flaticon.

[1] Including Sri Lanka

Table of Contents

Acronyms

AI	Artificial Intelligence
AIS	Automatic Identification System
AML	Anti-Money Laundering
AML/CFT	Anti-Money Laundering / Combating the Financing of Terrorism
ASEAN	Association of Southeast Asian Nations
BO	Beneficial Ownership
CFT	Combating the Financing of Terrorism
CPF	Countering Proliferation Financing
DeFi	Decentralized Finance
DLT	Distributed Ledger Technology
DNFBPs	Designated Non-Financial Businesses and Professions
DPRK	Democratic People's Republic of Korea
ERC	Ethereum Request for Comment (e.g., ERC-20 tokens)
ETH	Ethereum
EU	European Union
FATF	Financial Action Task Force
FICG	Financial Intelligence Consultative Group
FIU	Financial Intelligence Unit
FTZs	Free Trade Zones
GISIS	Global Integrated Shipping Information System
HS	Harmonized System (Codes)
ICIJ	International Consortium of Investigative Journalists
IMO	International Maritime Organization
IT	Information Technology
MERs	Mutual Evaluation Reports

NFTs	Non-Fungible Tokens
NGO	Non-Governmental Organization
NPO	Non-Profit Organization
NRA	National Risk Assessment
PESTLE	Political, Economic, Social, Technological, Legal, and Environmental
PF	Proliferation Financing
PPPs	Public–Private Partnerships
RUSI	Royal United Services Institute
SARs	Suspicious Activity Reports
SEZs	Special Economic Zones
SOEs	State-Owned Enterprises
STRs	Suspicious Transaction Reports
STS	Ship-to-Ship (Transfers)
TBML	Trade-Based Money Laundering
TFS	Targeted Financial Sanctions
UBO	Ultimate Beneficial Owner
UN	United Nations
UNICRI	United Nations Interregional Crime and Justice Research Institute
UNODC	United Nations Office on Drugs and Crime
UNSC	United Nations Security Council
US	United States (as used in “United States dollars”)
USDC	United States Dollar Coin
VA	Virtual Assets
VASPs	Virtual Asset Service Providers
WMD	Weapons of Mass Destruction

Introduction

The financing of the proliferation of weapons of mass destruction (WMD), nuclear, chemical, and biological weapons and their means of delivery, represents one of the most severe threats to international peace and security. **Countering proliferation financing (CPF) has thus become a critical pillar of the global security architecture.** Southeast Asia, with its dynamic economies, strategic maritime geography, and central position in global supply chains, finds itself at a unique and challenging nexus of PF risk. The region's economic strengths—its bustling ports, extensive trade networks, and growing manufacturing sectors—can be exploited by state and non-state actors seeking to procure materials, technology, and funds for WMD programmes.

The United Nations Security Council (UNSC) and the Financial Action Task Force (FATF) established a robust framework of obligations for states to prevent, detect, and disrupt PF activities. However, the effective implementation of these standards is a complex undertaking that requires a deep understanding of the specific threats and vulnerabilities present within a given jurisdiction or region.

This Handbook is based on the findings of a regional conference, which brought together stakeholders from Indonesia, Cambodia, Malaysia, Vietnam, Brunei Darussalam, Lao PDR, Sri Lanka, the Philippines and Thailand in Bangkok, Thailand, on 7 and 8 October 2025. The document outlines the deliberations of three working groups (Group A, Group B, and Group C) that collectively identified the primary PF threats, vulnerabilities, NRA process, challenges, best practices and necessary remedial actions for the region. Their findings provide an invaluable, on-the-ground perspective that moves beyond theoretical frameworks to address tangible, real-world challenges.

Participants at the Regional Conference on Proliferation Financing Risks in Southeast Asia

The objective of this handbook is to synthesize and expand upon the conference findings and provide a practical handbook and a catalogue of PF risks, thus enabling a robust understanding of the CPF landscape in Southeast Asia. It is structured as follows:

PART 1

delves into the specific PF **THREATS** impacting the region, as identified by the workshop participants. This section gives special attention to both traditional threats, such as the trade in dual-use goods, and emerging typologies, including the exploitation of virtual assets.

PART 2

analyzes the systemic **VULNERABILITIES** that enable and exacerbate these threats. It draws heavily on the consensus view from the working groups regarding legislative gaps, coordination failures, and a lack of transparency and awareness.

PART 3

elaborates on the **PF NRA PROCESS** in order to provide guidance and share experiences about this important exercise. This part is intended to aid jurisdictions that have not started their own yet.

PART 4

outlines the **CHALLENGES** and **BEST PRACTICES** observed in Southeast Asia.

EU P2P
Export Control Programme
for Dual-use Goods

CBRN
Centres
of Excellence
An initiative of the European Union

EU AML / CFT
GLOBAL FACILITY

APG
Asia/Pacific Group
on Money Laundering

Part 1: Proliferation Financing Threats in Southeast Asia

Funded by
the European Union

Part 1: Proliferation Financing Threats in Southeast Asia

The plenary session during the conference provided a clear and concerning picture of the specific PF threats confronting Southeast Asia. The region is not merely a passive transit point but an active environment where key elements of global proliferation networks operate. The threats identified by the working groups are not theoretical; they are tangible risks rooted in the region's economic structure, geography, and increasing integration into the digital economy.

1.1 Overview of the Regional Threat Environment: Exploiting Legitimate Commerce

1.1.1 SOUTHEAST ASIA AS A TRANSSHIPMENT HUB AND ILLICIT TRADE CORRIDOR

Participants identified the **risk of being a hub for illicit trade** as a main threat. This is arguably the most significant PF risk for the region. Southeast Asia is home to some of the world's busiest ports (e.g., Singapore, Port Klang in Malaysia, Laem Chabang in Thailand) and shipping lanes (e.g., the Strait of Malacca). This immense volume of container traffic provides a veil of anonymity for illicit shipments. Proliferation networks exploit this by:

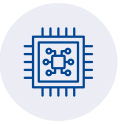
Transshipment and Re-export: Goods, including controlled dual-use items, can be shipped to a regional hub, repackaged, and re-exported with false documentation (e.g., changed bills of lading, fraudulent end-user certificates) to obscure their true origin and destination. This conceals the involvement of sanctioned states like the Democratic People's Republic of Korea (DPRK).

Commingling: Illicit goods can be hidden within legitimate consignments, making detection by customs authorities extremely difficult without specific, actionable intelligence.

Maritime Exploitation: The maritime sector is heavily exploited. Threats include ship-to-ship transfers to obscure the origin/destination of goods, falsifying shipping documents, and the use of oil and gas vessels for transporting dual-use items.

1.1.2 THE MANUFACTURE AND TRADE OF DUAL-USE GOODS

A critical threat, identified by participants as manufacture of dual-use items and as trade of dual-use items, is the region's role in the **supply chain for dual-use goods**. These are items and technologies that have legitimate commercial applications but can also be used in WMD programmes. Examples relevant to the region's industrial base include:



Electronics and Components: High-speed switches, capacitors, and transistors used in consumer electronics can also be used in missile guidance systems and nuclear triggers.

Machinery and Materials: Certain types of vacuum pumps, frequency converters, high-strength metals, and carbon fiber have applications in both civilian industry and uranium enrichment or missile manufacturing.

Chemicals: Precursor chemicals used for fertilizers or pharmaceuticals can also be used to produce chemical weapons.

Trade-Based Money Laundering (TBML): *Participants identified TBML as a significant threat, utilizing techniques such as* ***commodity misclassification*** *and* ***misdeclarations*** *(over- or under-valuation of goods) to move value across borders illegally.*

1.1.3 CIRCUMVENTION OF EXPORT CONTROL

Proliferation networks employ sophisticated strategies specifically designed to e**xploit weaknesses in export control systems**. Procurement agent networks operate by establishing seemingly legitimate commercial entities that approach manufacturers and distributors without disclosing the true end-user or end-use, allowing controlled items to be acquired under false commercial pretenses. These networks engage in specification manipulation, crafting procurement requests that fall just below control thresholds, for instance, requesting vacuum pumps with capabilities slightly below the pressure levels that would trigger licensing requirements, then modifying them post-delivery. Triangulation through third countries is commonplace: controlled items are legally exported to jurisdictions with minimal export controls, then re-exported to sanctioned destinations without the originating country's knowledge. Proliferators also exploit licensing gaps by breaking large orders into multiple small shipments over time, each below reporting thresholds, or by deliberately misclassifying goods using Harmonized System (HS) codes[1] for similar but uncontrolled items.

1.1.4 DIPLOMATIC AND STATE-SPONSORED CHANNELS

"Diplomatic relations with DPRK and Iran" were identified as pointing to a sophisticated and challenging threat. Sanctioned states, particularly the DPRK, have a long history of using their diplomatic and commercial infrastructure abroad to facilitate illicit activities. This includes:

Diplomatic Cover: Using diplomatic pouches, personnel, and premises to move cash, luxury or sensitive goods, or facilitate illicit deals, exploiting the protections afforded by the Vienna Convention on Diplomatic Relations.

State-Owned Enterprises (SOEs): Operating SOEs in sectors like shipping, construction, and trading in Southeast Asian countries to generate revenue and procure goods for WMD programmes. These entities can act as fronts, obscuring their connection to the sanctioned state.

Co-opting Nationals: Recruiting local nationals to act as facilitators, company directors, or financial intermediaries, further obscuring the network's true ownership and purpose.

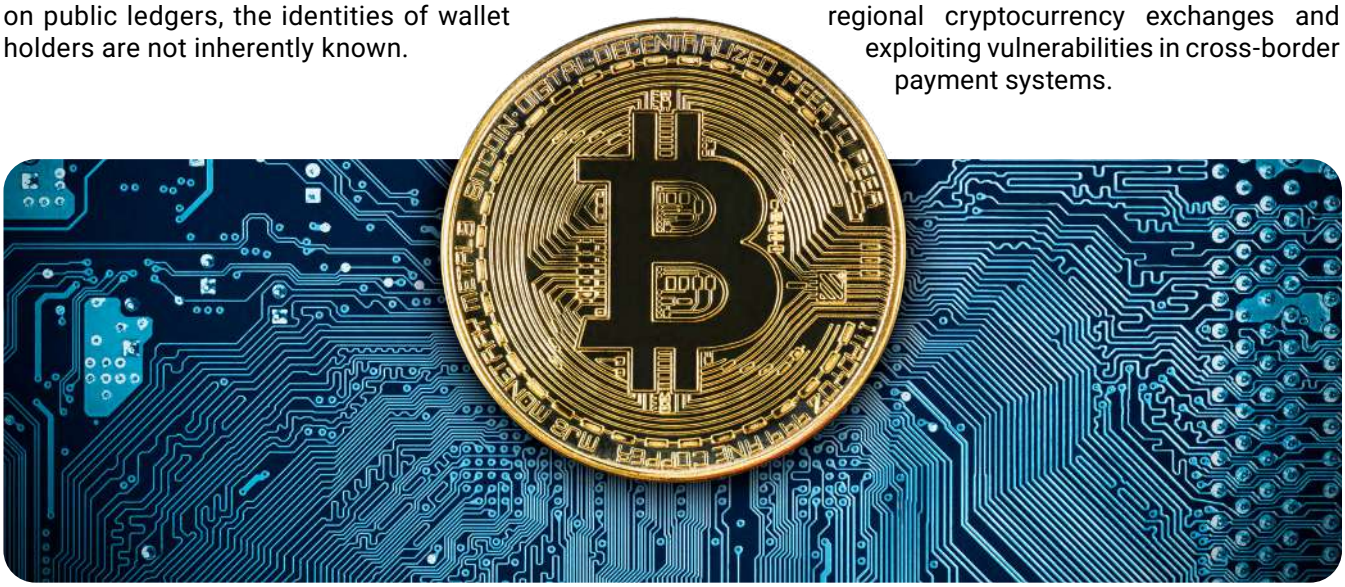
It was agreed that this threat is particularly difficult to counter as it involves sensitive diplomatic relationships and requires a high degree of intelligence-led investigation to distinguish legitimate state activity from illicit PF conduct.

[1] **Harmonized System (HS) Codes**: An internationally standardized numerical method of classifying trade products, developed by the World Customs Organization (WCO). These codes consist of a six-digit root used globally to identify goods for customs purposes, determine tariff rates, and monitor international trade compliance.

1.2 Emerging Threats and Non-Traditional Channels

1.2.1 THE MISUSE OF VIRTUAL ASSETS AND CRYPTOCURRENCIES

Virtual assets, as defined by the Financial Action Task Force (FATF), are digital representations of value that can be digitally traded, transferred, and used for payment or investment purposes, existing only in electronic form and recorded on distributed ledger technology (DLT), such as blockchain networks. The fundamental characteristics of virtual assets create what security analysts term a "value proposition" for illicit actors: speed and global reach, enabling transactions to be settled in minutes rather than days and sent anywhere in the world without traditional financial intermediaries. Another key feature is pseudonymity - while transactions are recorded on public ledgers, the identities of wallet holders are not inherently known.



These characteristics have fundamentally transformed the proliferation financing landscape, providing state and non-state actors with unprecedented capabilities to circumvent traditional financial controls and sanctions regimes. For proliferation financing actors, virtual assets offer two primary advantages: sanctions evasion, as VAs operate outside the traditional financial system and allow actors to **bypass the chokepoints** where sanctions are typically enforced, and direct revenue generation, where the VA ecosystem itself can be targeted for theft, creating **immediate sources of revenue** for proliferation activities.

The scale and sophistication of virtual asset misuse in proliferation financing is exemplified by the DPRK, which has transformed from a traditional sanctions evader into what is characterized as a "state-sponsored cybercriminal enterprise". For the DPRK regime, virtual assets are not merely tools for evasion but have become a **critical lifeline for financing weapons development programmes**, especially ballistic missile program financing comes from cyber activities involving virtual assets.

DPRK cryptocurrency operations represent the most sophisticated and persistent threat in this domain. These operations encompass multiple vectors including direct exchange hacking, deployment of malicious IT workers, and complex money laundering schemes that exploit regional cryptocurrency infrastructure. The Lazarus Group, a cybercrime group with strong links to the DPRK, and affiliated entities have demonstrated expertise in targeting regional cryptocurrency exchanges and exploiting vulnerabilities in cross-border payment systems.

The identification of "cryptocurrency trade" and the "rapid growth of virtual assets" as major threats is one of the most significant findings of the conference. Virtual assets offer several advantages to proliferation networks, especially those linked to the DPRK, which is a known pioneer in their malicious use:

Sanctions Evasion and Revenue Generation: State-sponsored hacking groups can steal vast sums of cryptocurrency from exchanges and individuals worldwide. These stolen funds are then laundered through a complex series of transactions to convert them into fiat currency, providing a vital source of untraceable revenue for WMD programmes, completely bypassing the formal banking system and its TFS obligations.

Procurement Payments: Virtual assets can be used to pay for illicitly procured goods and services in the underground markets. Their speed and cross-border nature allow for near-instantaneous payments to suppliers anywhere in the world, without routing through correspondent banks that would screen transactions against sanctions lists.

Anonymity and Obfuscation: While blockchain transactions are recorded on a public ledger, techniques like using privacy-enhancing coins (e.g., Monero), tumblers/mixers (which pool and mix coins from different sources to break the transaction trail), and chain-hopping (rapidly converting between different cryptocurrencies) make it exceptionally difficult for law enforcement to trace the flow of funds from their illicit origin to their ultimate destination.

Illicit generation of revenue through cyberactivities

139. In February, a cybersecurity firm reported[150] that State-sponsored cyberactors of the Democratic People's Republic of Korea, such as the Lazarus Group,[151] were responsible for nearly $1.7 billion worth of cryptocurrency theft in 2022, more than three times the amount that they stole in 2021 (see figure XXVII). The firm further assesses that the country is prioritizing cryptocurrency hacks "to fund its nuclear weapons programs". Of the total amount stolen by Democratic People's Republic of Korea cyberthreat actors in 2022, almost two thirds (approximately $1.1 billion) originated from attacks targeting decentralized finance platforms, including the Harmony Bridge[152] and Axie Infinity's Ronin network hacks.[153] [154] Similarly, according to a media report in May based on a separate cybersecurity company's analysis,[155] the Democratic People's Republic of Korea targets virtual assets of multiple Member States' companies "to obtain the foreign currency that it uses for its missile program", stealing $2.3 billion in cryptocurrency from 2017 to 2022. A Member State official assessed in May that the malicious cyberactivities of the Democratic People's Republic of Korea fund half of its missile programme.[156] [157]

REF : 1718 UN PANEL OF EXPERTS, REPORT S/2023/656 12 SEPT 2023

The 1718 UN Panel of Experts explicitly refers to cases of sophisticated money laundering through virtual assets. The report specifically names two major heists that exemplify the DPRK's focus on decentralized finance. Here are the details of those cases:

1. The Axie Infinity Ronin Network Hack (March 2022)

Axie Infinity is a very popular "play-to-earn" online video game that uses non-fungible tokens (NFTs). It runs on the Ronin network, which is a "sidechain" connected to the main Ethereum blockchain. This sidechain was created to make transactions faster and cheaper for players. The Ronin Bridge is the specific tool that allows users to move their cryptocurrency between the Ronin network and the Ethereum network.

The Lazarus Group orchestrated the attack. They used a sophisticated social engineering scheme, targeting a senior engineer at Sky Mavis (the company behind Axie Infinity) with a fake job offer. This allowed them to install malware and gain access to the company's systems. They eventually managed to gain control of five of the nine private security keys that validate transactions on the Ronin network. With this majority control, they were able to authorize two massive, fraudulent withdrawals.

The attackers stole approximately **$625 million** worth of Ethereum (ETH) and USD Coin (USDC), making it one of the largest cryptocurrency heists in history.

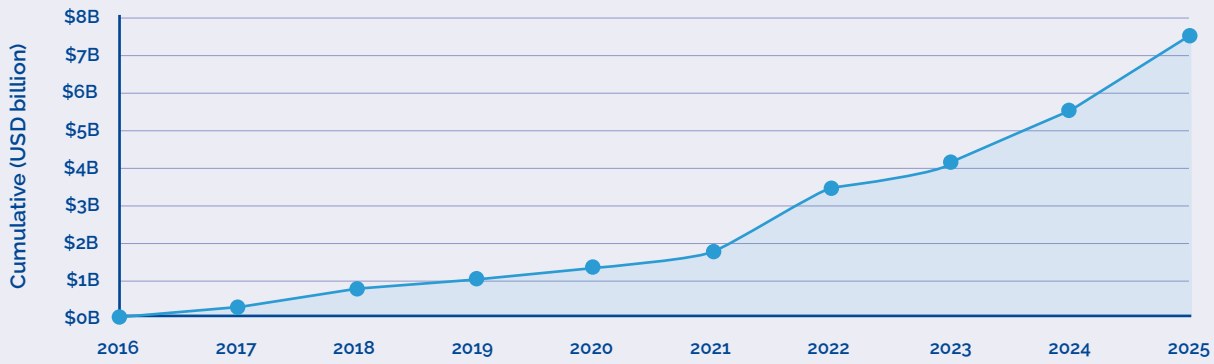
2. The Harmony Bridge Hack (June 2022)

Harmony is a blockchain platform designed for creating and using decentralized applications. Like Ronin, it has a "bridge" called the Horizon Bridge, which facilitates the transfer of crypto assets between the Harmony blockchain and other major networks like Ethereum and the Binance Smart Chain. These bridges are crucial for the interoperability of the DeFi ecosystem but are also complex and can be a single point of failure.

The Lazarus Group is also credited with this attack. They exploited a vulnerability in the security of the Horizon Bridge. The investigation revealed that the attackers were able to compromise the private keys that controlled the bridge's multi-signature wallet. This type of wallet requires multiple keys to approve a transaction for security, but the attackers managed to gain control of the required number of keys, allowing them to authorize the transfer of funds to their own wallets.

The attackers made off with approximately **$100 million** in various cryptocurrencies, including ETH, Tether, and Wrapped Bitcoin. The hack effectively drained the bridge of its assets, rendering it inoperable and causing significant financial losses for users who had funds locked in it.

These cases and others show that virtual assets have turned to be the major revenue generating market for DPRK. The sanctioned nation does not necessarily need to steal physical cash to get into financial markets, otherwise, they can hack into exchanges, bridges, NFT marketplaces and other intermediaries to gain substantial amounts of money. The upward trend is captured by Blockchain Analytics companies and the UN Panel of Experts in the following figure:



Sources: Chainalysis 2026 Crypto Crime Report; TRM Labs; UN Panel of Experts; U.S. Treasury/OFAC.

Operational Tip: Virtual Asset Tracing Tools

Public Blockchain Explorers (e.g., Etherscan, Blockchain.com)

Purpose: To view, search, and analyze transactions on public blockchains like Bitcoin and Ethereum. They are the fundamental tools for manual crypto tracing.

How to Use for PF Analysis:

- **Enter** a known illicit wallet address.
- **Trace** transactions across wallets.
- **Identify** mixers, bridges and high-risk services.
- **Track** funds to centralized exchanges.

Access:

- **Ethereum & ERC-20 Tokens:** etherscan.io
- **Bitcoin:** blockchain.com/explorer
- **Solana:** solscan.io

1.2.2 CYBER CRIME & AI-BASED ATTACKS

While one jurisdiction specifically listed this as a primary threat, the nature of digital crime makes it a borderless, regional concern. In the context of Proliferation Financing, this represents a shift from moving funds to generating illicit funds.

The specific mention of "AI-based attacks" by one participant indicates the awareness of the higher level of sophistication of these attacks. AI can be used to create highly convincing, localized phishing emails to steal credentials from bank employees or government officials.

1.2.3 ONLINE MARKETPLACES & THE "DUAL-USE" DILEMMA

This threat highlights a significant gap in traditional export controls, which were originally designed for large, bulk shipments (containers) rather than the high-volume, low-value parcels typical of e-commerce.

Unlike traditional trade, where exporters are often licensed and vetted, online marketplaces allow anonymous or 'fly-by-night' sellers. This anonymity aligns with the threat of "shell companies" and "misdeclarations", allowing proliferators to procure sensitive technology without revealing the true end-user.

> ***In conclusion, the PF threat landscape in Southeast Asia is multi-dimensional. It combines the large-scale, systemic risk of exploitation of the region's legitimate trade and shipping industries with sophisticated, state-sponsored operations and the agile, technologically advanced threat posed by virtual assets. The findings of the conference demonstrate a clear understanding that an effective CPF strategy must be capable of addressing all these facets simultaneously.***

EU P2P
Export Control Programme
for Dual-use Goods

CBRN
Centres
of Excellence
An initiative of the European Union

EU AML / CFT
GLOBAL FACILITY

APG
Asia/Pacific Group
on Money Laundering

Part 2: Proliferation Financing Vulnerabilities in Southeast Asia

Funded by
the European Union

Part 2: Proliferation Financing Vulnerabilities in Southeast Asia

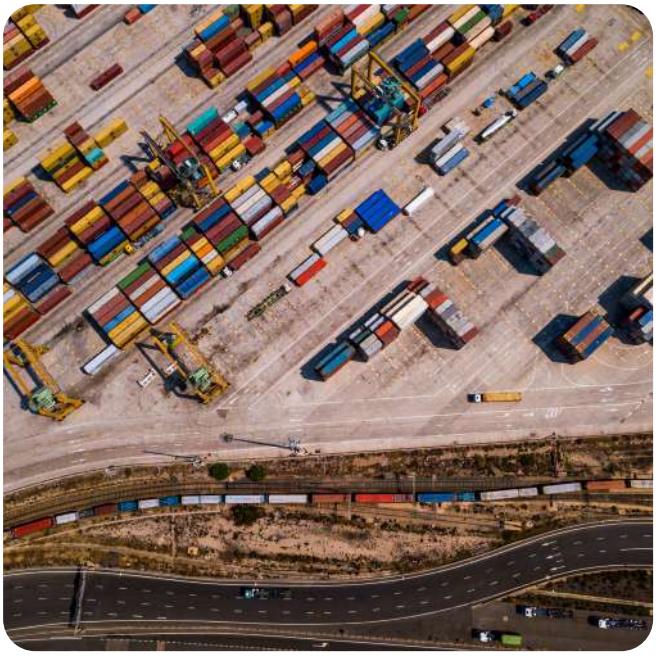
The identification of threats is only the first step in the Counter-Proliferation Financing (CPF) cycle. During the conference, the working groups engaged in a rigorous self-assessment, moving beyond surface-level observations to identify the structural, legal, and operational deficiencies that characterize the current regional landscape.

The conversations held across the three groups identified eight key vulnerabilities pertinent to the ASEAN region. These are discussed in turn.

2.1 Weak and uneven Cryptoassets and Virtual Asset regulatory frameworks

Across Southeast Asia, regulatory frameworks for virtual assets remain uneven. Several jurisdictions lack comprehensive supervision of VASPs, while knowledge gaps among regulators, financial institutions, and law enforcement agencies create significant detection challenges. Virtual assets continue to be exploited for anonymized cross-border transfers, raising PF exposure.

Reflecting the threat analysis, participants pointed to the "limited specific regulation" regarding virtual assets. While the FATF recommendations 15 and 16 require the regulation of VASPs and adoption of the travel rule, implementation in the region is highly asymmetrical. Some jurisdictions have banned VAs entirely, while others have allowed a proliferation of exchanges with minimal AML/CFT/CPF oversight.



2.2 Maritime Sector, FTZs, and SEZs

Southeast Asia's vast maritime networks, busy ports, and multiple free trade zones create inherent vulnerabilities. Complex supply chains, ship-to-ship transfers, and weak cargo verification mechanisms enable sensitive goods to transit with limited scrutiny. Export-control oversight varies significantly across Special Economic Zones.

Some participants introduced a critical concept regarding "lack of supervision in certain zones". This refers to the industrial parks, Free Trade Zones (FTZs), and Special Economic Zones (SEZs) that are prevalent across Southeast Asia. These zones are economic engines designed to attract foreign direct investment through tax breaks and, crucially, simplified customs procedures. There was a consensus that "simplified" oversight creates a permissive environment for PF. In many of these zones, goods can be imported, assembled, repackaged, and re-exported with minimal physical inspection or documentation checks.

The sheer volume of transshipment traffic in the region's mega-ports means that authorities rely heavily on risk profiling rather than physical inspection. If the risk profiling algorithms are not updated with specific PF indicators (e.g., specific dual-use HS codes, known procurement front companies), the vast majority of illicit cargo will pass through these hubs unchallenged.

Operational Tip: Maritime and Vessel Analysis Tools

MarineTraffic: Live tracking of vessels worldwide using Automatic Identification System (AIS) data.

How to Use for PF Analysis:

- Monitor port areas and key shipping lanes (like the Strait of Malacca) for unusual vessel movements.
- Identify a vessel's current location, reported destination, and basic details (flag, size).
- Screen vessels against known names or IMO numbers (a unique 7-digit identifier that never changes) from intelligence reports or sanctions lists in real-time.

www.marinetraffic.com

IMO Global Integrated Shipping Information System (GISIS): Database for vessel and company information maintained by the International Maritime Organization.

How to Use for PF Analysis:

- Use the IMO number to verify a vessel's identity and history.
- Look up the registered owner, manager, and operator of a vessel of interest to identify links to shell companies or sanctioned entities.
- Check the "History of Name/Flag" section to identify frequent changes ("flag hopping"), a key red flag for sanctions evasion.

gisis.imo.org/Public/ (Requires free registration)

Export Control Enforcement Gaps in Special Economic Zones

A critical but often overlooked vulnerability within Free Trade Zones and Special Economic Zones is the systematic **exemption from normal export licensing procedures** and the provision of simplified customs formalities that were designed to facilitate legitimate trade but inadvertently create export control loopholes. In many Southeast Asian FTZs, goods can enter, be stored, assembled, manufactured, repackaged, and re-exported with minimal documentation requirements and without triggering the standard export control review processes that would apply in the broader customs territory. This creates an environment where dual-use goods can be imported as components, assembled into controlled items (such as precision machine tools or specialized pumps), and re-exported without ever being subjected to export license scrutiny. The "light touch" regulatory approach in these zones—intentionally designed to reduce bureaucratic barriers for investors—means that export control authorities often have limited visibility into or jurisdiction over activities occurring within zone boundaries.

2.3 Informal Financial Channels

The prevalence of hawala-style networks, cash-based economies, and unregistered money service businesses allows cross-border transfers to occur outside formal reporting frameworks. These informal channels continue to be exploited by illicit actors due to low transparency and minimal regulatory visibility. "Informal financial networks" was singled out as a financial system vulnerability and points to another channel that operates outside the purview of formal regulation. Networks such as hawala or other similar informal value transfer systems are prevalent in many parts of Southeast Asia. They rely on trust and ethnic or family connections to move value across borders without moving money physically. While most of their use is for legitimate remittances, their lack of record-keeping and regulatory oversight makes them vulnerable to misuse for financing illicit activities, including PF, on a smaller scale. They can be used for the final leg of a financing scheme, paying local agents or facilitators in a way that leaves no formal paper trail.

2.4 Weak Regulatory and Legislative Frameworks

Some jurisdictions have yet to explicitly criminalize proliferation financing, while others maintain only partial or outdated enforcement mechanisms. Export-control regimes, including dual-use goods lists, remain insufficient in several countries. Weak oversight of ship registries further compounds the challenge.

Many jurisdictions in the region suffer from "regulatory gaps" where PF is not distinctively criminalized or is conflated with terrorist financing. Unlike money laundering, which deals with the proceeds of crime, PF often involves funds from legitimate sources (e.g., state budgets or legitimate trade revenue) used for illicit ends. Discussions revealed that without specific PF legislation, authorities often lack the legal standing to investigate financial flows that do not have an obvious predicate criminal offense attached to them. This legislative void means that even if intelligence identifies a suspicious flow of funds related to a dual-use procurement, law enforcement may be powerless to seize assets or prosecute the actors involved unless a direct link to a sanctioned entity can be proven immediately—a high bar in the early stages of an investigation.

A critical operational vulnerability was identified: the "absence of a nationally adopted list of dual-use goods." This is a foundational gap. In many Southeast Asian nations, export control laws focus primarily on military hardware (munitions lists). Dual-use items—goods with both civilian and military applications, such as carbon fiber, high-precision gyroscopes, or certain chemical precursors—often fall into a legal grey area.

Without a gazetted, legally binding control list (aligned, for instance, with the Wassenaar Arrangement or EU control lists), customs officials and the private sector are left without a clear definition of what constitutes "contraband" in the context of PF. This creates a situation where "enforcement clarity" is compromised; customs officers cannot detain a shipment of high-spec vacuum pumps if the law does not explicitly define them as controlled items, effectively granting proliferators a legal channel for procurement.

Operational Tip: Trade Data and Dual-Use Goods Analysis Tools

UN Comtrade Database

Purpose: A repository of official international trade statistics, allowing detailed analysis of global trade flows.

How to Use for PF Analysis:

- Analyze trade flows with high-risk countries.
- Detect unusual trade patterns.
- Monitor dual-use goods using HS codes.

comtrade.un.org

International Export Control Regime Lists

Purpose: Official lists of controlled dual-use and military goods. These are reference documents, not search tools, but are essential for identifying what to look for.

How to Use for PF Analysis:

- Train stakeholders on controlled goods.
- Cross-check technical specifications.
- Match goods with relevant HS codes.

Access:

- Wassenaar Arrangement Lists: **wassenaar.org/control-lists**
- EU Dual-Use Control List: Available via the EU's official journal.

2.5 Information Sharing and Cooperation Gaps

Perhaps the most pervasive vulnerability, cited by all groups at the conference, is the lack of effective inter-agency coordination. Inter-agency coordination remains fragmented in many jurisdictions. Limited intelligence sharing between customs, FIUs, law enforcement, and regulatory agencies inhibits timely PF detection. Regionally, cooperation is still evolving, and engagement of private-sector actors, especially DNFBPs, is inconsistent creating considerable vacuum within which PF threats can thrive.

"Inter-agency coordination" was identified as a primary vulnerability, noting that agencies often operate in "silos." In practice, this means that data sits isolated. The Customs department may hold data on a suspicious shipment of electronics to a high-risk jurisdiction, while the FIU holds data on a suspicious wire transfer from a shell company in the same timeframe. Separately, these data points might not trigger an alarm; combined, they constitute a clear PF typology.

There is often no established legal gateway or operational mechanism for these agencies to share data in real-time. The absence of a "fusion center" or a standing national task force means that information sharing is often ad-hoc, reactive, and too slow to intercept a shipment or freeze a transaction before it clears.

2.6 Geographic Exposure

Proximity to the DPRK and extensive coastlines create opportunities for evasion through illicit maritime activity. Numerous small ports, archipelagic geography, and porous borders make monitoring and interdiction challenging. This exposure is exacerbated by "maritime security vulnerabilities" and "cross-border control weaknesses", which noted that the sheer volume of small ports and porous borders impedes effective oversight. Furthermore, it was emphasized that the lack of supervision in specific zones increases the risk of the region serving as a "hub for illicit trade." Consequently, the archipelagic geography not only facilitates evasion through illicit maritime activity but also complicates the inter-agency coordination and enforcement efforts necessary to monitor these transit points effectively.

2.7 Awareness and Capacity Constraints

The observation that PF awareness remains low was substantiated by participants, including identifying gaps in "outreach to the private sector" as a critical vulnerability. This lack of awareness is compounded by the "complexity of PF typology", which creates significant hurdles for frontline operators attempting to identify illicit activity. To address these deficiencies, some participants emphasized the urgent need for capacity building and specific training programmes, particularly given the "regulatory and legal gaps" in current enforcement frameworks.

In short, PF awareness remains low across public and private sectors. Many frontline operators lack training in dual-use goods, sanctions evasion, or PF typologies. Resource constraints impact FIUs, customs, and export control agencies.

2.8 Beneficial Ownership Transparency

Weak beneficial ownership (BO) registries, limited verification practices, and extensive use of nominee arrangements facilitate the misuse of legal structures by proliferators. Shell and front companies remain common tools for obscuring financial and trade activity.

A strong emphasis was placed on "lack of transparency in beneficial ownership" and "company registration." This vulnerability strikes at the heart of how PF networks operate. In several Southeast Asian jurisdictions, as is the case in different parts of the world, it remains far too easy and inexpensive to register a limited liability company; the risk of exploiting these features will intensify without the proper beneficial ownership information requirements. Proliferators may use networks of clone shell companies—entities with no physical presence or significant operations—to act as source and destination contracting parties for illicit trade. One of the working groups noted that the lack of rigorous verification during the company formation process allows actors to use "straw men" or nominee directors to hide the ultimate beneficial owner (UBO).

Operational Tip: Corporate Structure and Beneficial Ownership Tools

OpenCorporates: The world's largest open database of company information, aggregating data from official national registries.

How to Use for PF Analysis:

- Search for a suspected front company to find its jurisdiction, registration status, and registered address.
- Identify the names of directors and officers. Search these names again to see if they are linked to dozens or hundreds of other companies, a sign of a professional nominee service used to obscure ownership.
- Map out networks of related companies to uncover the larger structure of a procurement network.

opencorporates.com

ICIJ Offshore Leaks Database: A searchable database of information from major offshore leaks like the Panama Papers, Paradise Papers, and Pandora Papers.

How to Use for PF Analysis:

- Search for names of individuals, companies, or addresses linked to a suspicious transaction or entity.
- Uncover previously hidden links between public officials, sanctioned individuals, and the offshore companies they use to hold assets or conduct business.
- This is a powerful tool for piercing corporate secrecy and identifying ultimate beneficial owners.

offshoreleaks.icij.org

One group mentioned that Non-Profit Organizations (NPOs) and charities are susceptible to abuse by malicious actors who exploit the sector's high public trust and complex global cash flows to disguise illicit activities. These organizations can serve as financial conduits, where funds ostensibly raised for humanitarian aid are diverted or commingled to finance terrorism or weapons proliferation. A significant vulnerability lies in cross-border operations, where a legitimate NPO may unwittingly engage a local partner NGO that maintains concealed affiliations with sanctioned entities or designated groups, effectively allowing these actors to bypass international financial controls and access funding under the guise of charitable work.

EU P2P
Export Control Programme
for Dual-use Goods

CBRN
Centres
of Excellence
An initiative of the European Union

EU AML / CFT
GLOBAL FACILITY

APG
Asia/Pacific Group
on Money Laundering

Part 3: The Proliferation Financing National Risk Assessment Process

Funded by
the European Union

Part 3: The PF NRA Process

A comprehensive, step-by-step National Risk Assessment (NRA) process methodology is essential because proliferation financing risk assessment remains an emerging discipline with limited standardized guidance compared to more mature areas like anti-money laundering or counter-terrorism financing. Most jurisdictions are conducting their first or second PF NRA and may lack institutional experience in threat identification, vulnerability analysis, and risk prioritization specific to WMD proliferation networks. Without granular procedural guidance—covering everything from initial scoping and stakeholder identification to data collection instruments, analytical frameworks, and risk rating methodologies—countries risk producing assessments that are overly generic, fail to capture jurisdiction-specific threats, or cannot translate findings into actionable policy reforms. Therefore, a detailed methodology section is described hereinafter. It should be cautioned that this part is not a prescription but an endeavor to help jurisdictions follow a guided path in conducting their NRA.

Phase One: Establishing Governance and Defining Scope

Objective: The foundation of any successful proliferation financing National Risk Assessment requires establishing the necessary institutional architecture and mandates to ensure a comprehensive, multi-sectoral evaluation of national proliferation financing risks.

STEP 1.1: SECURING HIGH-LEVEL POLITICAL MANDATE

The first critical step involves obtaining formal authorization from the highest political levels through a presidential decree, ministerial order, or legal clause that officially mandates the conduct of the proliferation financing NRA. The mandate must clearly specify the legal authority to collect data from all relevant sectors, the mandatory nature of cooperation from all government entities, a realistic timeline for completion, and the allocation of dedicated resources including both budget and personnel. Without this formal authorization, technical teams often encounter institutional resistance, data access barriers, and competing priorities that derail the assessment process.

STEP 1.2: FORMING THE NATIONAL STEERING COMMITTEE

The FIU or an inter-governmental committee typically serves as the central coordinator, bringing together high-level representatives from the Ministry of Foreign Affairs, export control agencies, customs administration, maritime authorities, law enforcement agencies, regulatory bodies (central bank, securities authority, supervisors of non-financial sectors), the Ministry of Industry or Trade, and private sector representatives including banking associations, chambers of commerce, and shipping associations.

The steering committee operates according to a formal charter that defines its composition, establishes

meeting frequency (typically monthly at minimum), clarifies decision-making authority, sets out escalation mechanisms, and establishes confidentiality requirements. Inter-agency data sharing agreements provide the legal and operational framework for information exchange throughout the assessment process.

STEP 1.3: ESTABLISHING TECHNICAL WORKING GROUPS

Each participating agency designates technical liaison officers who form specialized teams: a data collection team, an analysis and assessment team, a private sector engagement team, and a drafting and documentation team. A lead project coordinator, usually from the FIU, develops a detailed project plan with a Gantt chart showing tasks, deadlines, and dependencies, maintains a risk and issue register, and implements an internal communications plan.

STEP 1.4: DEFINING ASSESSMENT SCOPE

The scoping exercise addresses geographic coverage (entire national territory and/or special economic zones) and sectoral coverage. The financial sector typically includes banks, insurance companies, securities markets, and money remittance services. Designated non-financial businesses and professions encompass accountants, lawyers, and dealers in precious metals and stones. Trade sectors include import/export operations, maritime shipping, air freight, and land transport. High-risk industrial sectors particularly include semiconductors, chemicals, precision machinery, nuclear technology, and aerospace, if present.

The assessment prioritizes specific threats based on national context, typically the North Korean and Iranian nuclear and missile programmes, plus any relevant proliferation concerns. The scoping document should articulate the assessment's objectives, specify covered sectors and threats, identify any exclusions, describe the methodology (typically FATF methodology or any other one such as RUSI), and establish evaluation criteria and key indicators.

Phase Two: Data Collection and Stakeholder Engagement

Objective: This phase gathers comprehensive and reliable data from multiple quantitative and qualitative sources to build a complete picture of national proliferation financing risks, balancing breadth of coverage with depth of analysis.

STEP 2.1: DESIGNING DATA COLLECTION TOOLS

Tailored questionnaires are designed for each stakeholder category. Law enforcement questionnaires probe proliferation financing-related investigations, types of crimes detected, observed patterns, investigative capabilities and gaps, and international cooperation issues. Regulatory body questionnaires address the legal and regulatory framework, supervision programmes, sanctions imposed, training provided and identified gaps. Financial institution questionnaires capture high-risk transactions, suspicious transaction reports related to proliferation financing, internal policies, screening systems, awareness levels, and challenges in identifying red flags. Trade sector questionnaires gather data on trade volumes with countries of concern, types of goods traded (especially dual-use items), payment mechanisms, transshipment points, and customer due diligence practices.

STEP 2.2: DISTRIBUTING QUESTIONNAIRES AND COLLECTING QUANTITATIVE DATA

Questionnaires are distributed with cover letters emphasizing importance and confidentiality, with clear deadlines (typically four to six weeks) and designated contact persons. Data collection extends beyond questionnaires to statistical sources including suspicious transaction reports from the FIU, export license applications and refusals from customs and export control authorities, cross-border wire transfers and trade finance data from financial institutions, and ship registration and port traffic data from maritime authorities.

STEP 2.3: CONDUCTING QUALITATIVE CONSULTATION SESSIONS

Sectoral workshops bring together fifteen to twenty participants from similar industries to discuss shared challenges. One-on-one expert interviews provide in-depth discussion with sanctions compliance officers, export control experts, and specialized investigators. Government roundtables bring together different agencies with complementary perspectives. Discussion agendas probe observed patterns, capability gaps, control effectiveness, implementation challenges, training needs, and best practices.

STEP 2.4: GATHERING OPEN-SOURCE INFORMATION

A comprehensive political, economic, sociological, technological, legal and environmental (PESTLE) analysis examines the national context across political, economic, social, technological, legal, and environmental dimensions. The research examines international case studies through UN Panel of Experts reports, detected violation cases globally, documented proliferation financing patterns, and National Risk Assessment reports from other countries. Public databases provide valuable indicators including UN Comtrade trade data, FATF MERs, and regional analyses.

STEP 2.5: DATA VALIDATION AND PROCESSING

Data quality checks verify completeness, consistency, and reliability. Missing or incomplete data is addressed through follow-up, appropriate statistical estimation, and careful documentation of limitations. Data organization involves standardizing formats, coding qualitative data, creating derived variables, and building a clean master database.

Phase Three: Risk Identification and Analysis

Objective: This phase systematically analyzes collected data to identify threats, vulnerabilities, and consequences according to FATF (or any other) methodology, remaining rigorous and evidence-based while accessible to non-technical audiences.

STEP 3.1: THREAT IDENTIFICATION

Threat analysis examines the likelihood and nature of attempts to use the national jurisdiction for proliferation financing. Program-related threats focus on specific proliferation programmes (North Korean and Iranian programmes). Geographic threats assess how physical location creates vulnerability through proximity, transit points, major ports or airports, and border areas with weak controls. Trade-related threats examine commercial relationships including direct trade volume with sanctioned countries, historical trading relationships, indirect trade patterns, and complex trading networks.

A threat assessment matrix evaluates likelihood (one to five scale), impact, priority (product of likelihood and impact), and documents supporting evidence. Geographic heat maps visualize threat distributions spatially.

STEP 3.2: VULNERABILITY ANALYSIS

Vulnerability analysis assesses internal weaknesses across four dimensions. Legal and regulatory vulnerabilities examine whether adequate frameworks exist to prevent and detect proliferation financing, including specific laws implementing UN Security Council resolutions and FATF TFS requirements, coverage of all proliferation financing forms, clear definitions for dual-use goods, and deterrent penalties. Institutional and operational vulnerabilities assess whether agencies possess implementation capacity, including training and resources, inter-agency coordination, information technology systems, and specialized experts.

Sectoral vulnerabilities examine specific industries. For financial institutions, assessment evaluates understanding of proliferation financing risks, screening

system quality, transaction monitoring effectiveness, and suspicious transaction report quality. For trade sectors, analysis assesses awareness levels, customer due diligence practices, freight forwarder capabilities, and customs oversight effectiveness.

OPTIONAL: STEP 3.3: CONSEQUENCE ASSESSMENT

Consequence assessment examines potential outcomes if risks materialize. Security consequences include contribution to the spread of WMD, undermining regional and international security, nuclear terrorism risks, and geopolitical stability effects. Economic consequences include international sanctions, loss of correspondent banking relationships, foreign direct investment decline, reputation damage, and investigation costs. Legal and reputational consequences include FATF grey list placement, negative international assessments, and erosion of international trust.

Phase Four: Risk Assessment and Prioritization

Objective: This phase integrates threats, vulnerabilities, and consequences into a comprehensive risk assessment and ranks risks by priority to guide resource allocation.

STEP 4.1: DEVELOPING THE RISK ASSESSMENT MODEL

The FATF methodology defines Risk as Threat × Vulnerability × Consequences. A unified rating scale (one to five) ensures consistency, where one indicates very low, two indicates low, three indicates medium, four indicates high, and five indicates critical. Aggregate risk levels translate scores into categories: (low risk), (medium risk), (high risk), (critical risk).

Sectoral risk assessment tables show threat rating, vulnerability rating, consequence rating, overall risk (product of the three), and risk classification for each sector. Risk heat maps and radar charts provide visual representations across sectors, regions, and risk dimensions.

STEP 4.2: PRIORITIZING RISKS

Risk prioritization ranks risks by overall score but refines ranking by considering treatability, available resources, and potential impact of mitigation measures. A prioritization matrix shows overall score, assigned priority, justification, and recommended actions. Consultation with the steering committee validates analytical prioritization.

An implementation roadmap organizes actions temporally: short-term priorities (zero to six months) address critical risks requiring immediate action, medium-term priorities (six to eighteen months) tackle high risks requiring capability development, and long-term priorities (eighteen to thirty-six months) address medium risks and structural reforms.

STEP 4.3: DEVELOPING MITIGATION STRATEGIES

For each high or critical priority risk, comprehensive mitigation strategies comprise legal and regulatory measures (legislative amendments, new regulations, sectoral guidance, enforcement procedures), institutional measures (capacity building, specialized training, recruitment, technology investments), operational measures (new procedures, information sharing protocols, coordination mechanisms, reporting standards), and collaborative measures (international partnerships, regional cooperation, private sector engagement, awareness programmes).

Phase Five: Drafting, Review, and Publication

Objective: This phase prepares the comprehensive final National Risk Assessment report, reviews it thoroughly, obtains approvals, and publishes it appropriately.

STEP 5.1: DRAFTING THE REPORT

The report structure includes an Executive Summary (five to ten pages) providing context, methodology, key findings, and recommendations. The Introduction (ten to fifteen pages) describes national context, legal framework, assessment scope, and methodology. The Context Analysis chapter (fifteen to twenty pages) presents PESTLE analysis, key industries, trade relationships, and infrastructure. The Threat Analysis chapter (twenty to twenty-five pages) identifies major threats with supporting evidence and quantitative assessments. The Vulnerability Analysis chapter (twenty-five to thirty pages) examines legal, institutional, sectoral, and transparency vulnerabilities. The Consequence Assessment chapter (fifteen to twenty pages) explores security, economic, legal, and reputational impacts. The Overall Risk Assessment chapter (twenty to twenty-five pages) presents matrices, heat maps, and prioritization. The National

Action Plan chapter (twenty-five to thirty-five pages) details mitigation strategies, actions, timelines, responsibilities, and indicators. Conclusions and Recommendations (ten to fifteen pages) synthesize key messages. Annexes provide supporting material.

STEP 5.2: INTERNAL REVIEW

The draft undergoes technical review (data accuracy, methodology, logic, completeness), legal review (legal accuracy, compliance, citations), security review (classification, public/classified versions), and quality assurance review (writing quality, formatting, charts).

STEP 5.3: STAKEHOLDER CONSULTATION

The draft is shared with steering committee members, contributing agencies, and potentially private sector representatives. A review workshop presents findings, discusses priorities, gathers feedback, and builds consensus. The team reviews feedback, identifies necessary changes, implements revisions, and documents decisions.

STEP 5.4: FORMAL APPROVAL

The final report is submitted to the steering committee, relevant ministries, and finally the Cabinet or competent authority for approval, with written approvals at each stage.

STEP 5.5: PUBLICATION AND DISSEMINATION

Different versions serve different audiences: full classified version (restricted), public version (sensitive information removed), executive summary (general public and media), and English version (international partners). An outreach program includes seminars, training workshops, parliamentary briefings, and awareness campaigns.

Phase Six: Monitoring and Updating

Objective: Monitoring ensures the National Risk Assessment remains relevant and that action plan implementation progress is tracked systematically.

STEP 6.1: ESTABLISHING MONITORING MECHANISMS

A permanent follow-up committee meets quarterly to review implementation progress, assess measure effectiveness, and identify emerging risks. A reporting system requires quarterly reports from responsible entities, annual comprehensive reports, and a dashboard tracking key indicators.

Monitoring indicators include compliance indicators (laws adopted, sectors covered, staff trained), effectiveness indicators (cases detected, assets frozen, convictions, suspicious transaction reports), and impact indicators (FATF assessments, sanctions indicators, international confidence).

STEP 6.2: PERIODIC UPDATING

Annual data updates gather new statistics, update risk assessments, and prepare progress reports. Comprehensive review every three to five years involves full reassessment, lessons learned incorporation, methodology updates, and reprioritization. Responsiveness to developments requires monitoring emerging risks, conducting rapid assessments when needed, and making emergency updates when circumstances change significantly.

EU P2P
Export Control Programme
for Dual-use Goods

CBRN
Centres
of Excellence
An initiative of the European Union

EU AML / CFT
GLOBAL FACILITY

APG
Asia/Pacific Group
on Money Laundering

Part 4: Challenges and best practice observed in Southeast Asia

Funded by
the European Union

Part 4: Challenges and best practice observed in Southeast Asia

4.1 Overview of the Regional Challenges faced in Southeast Asia

Effective implementation of a Counter-Proliferation Finance (CPF) program in Southeast Asia remains constrained by multiple structural, institutional, and operational challenges. Drawing on the engagement held with the three working groups as well as existing national risk assessments (NRAs) and regional analysis, including UNICRI's 2023 report, the following key obstacles have emerged:

LIMITED CASE STUDIES AND TYPOLOGY DEVELOPMENT

There is a lack of domestic PF-specific cases in many jurisdictions. Without a robust body of case studies, financial intelligence units (FIUs), law enforcement, and regulators struggle to analyze typologies, refine red-flag indicators, or build tailored risk-based frameworks.

In addition, as noted by participants, jurisdictions lack sufficient documented typologies to guide detection, which is an issue considering proliferators exploiting ever emerging PF channels, such as virtual assets exploitation for instance.

RELUCTANCE TO SHARE INFORMATION ACROSS AGENCIES

Several national authorities—including intelligence services, customs, export-control agencies, and FIUs—are reticent to share potentially sensitive information about suspected or confirmed proliferation finance activities.

This reticence impedes the identification of patterns, prevents strategic analysis, and weakens the development of preventive mechanisms, as highlighted in expert-level dialogues convened by EU P2P.

ABSENCE OF STRUCTURED DATA-SHARING MECHANISMS

Even where there is a willingness to cooperate, many states lack formal mechanisms to exchange intelligence, typologies, or best practices in a systematic manner. There is a notable gap in dedicated platforms or working groups to facilitate sharing of PF risk information, inter-agency engagement, or joint lessons-learned reviews.

The primary tool for data collection—questionnaires sent to the private sector—is plagued by questionnaire fatigue, resulting in low response rates. Even when responses are received, they are often superficial because respondents lack a deep understanding of the subject matter. Furthermore, current methodologies struggle to incorporate region-specific case studies. This leads to generic reports that fail to reflect the unique maritime and transit risks inherent to Southeast Asia.

---

[1] **The NRAs that were reviewed are:**

- **Indonesia**, available at: https://www.ppatk.go.id/backend/assets/uploads/20220412140054.pdf.
- **Malaysia**, available at: https://amlcft.bnm.gov.my/documents/6312201/6322762/PFRA_Report_Aug_2021.pdf/1adb8cd9-60fe-0b52-349c-10edef0fbcdb?t=1646270186806.
- **Thailand**, available at: https://www.amlo.go.th/amlo-intranet/media/k2/attachments/NRAYThailandYforYPublicationYEnglish_6112.pdf.

[2] **UNICRI, 'CBRN Proliferation Financing:** A Perspective from Southeast Asia - October 2023', 2023. Available online: https://unicri.org/Publication-CBRN-Proliferation-Financing-Perspective-from-Southeast-Asia.

LIMITED ENGAGEMENT BY DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONALS (DNFBPs)

DNFBPs, such as legal services, accounting firms, trust and corporate service providers, are often not fully integrated into CPF frameworks. This is partially due to low CPF awareness and a weak compliance culture in these sectors. Without their engagement, early-warning signals and red-flag reporting are less effective, leaving a blind spot in the national PF defense architecture.

RESOURCE CONSTRAINTS IN KEY AGENCIES

Several jurisdictions report insufficient financial and human resources for critical agencies. FIUs, customs, and export-control authorities frequently lack the specialized personnel and funding needed to do PF-specific work in addition to their general obligations. The process is further hindered by institutional memory loss. Frequent changes in points of contact within government agencies disrupt the continuity of the NRA process, slowing down knowledge transfer and often forcing new teams to start from scratch. Additionally, some participants noted that the process can devolve into a check-box trap—a compliance exercise aimed at satisfying FATF requirements rather than a genuine deep-dive into national security. This is exacerbated by a lack of meaningful consultation with critical private sectors, such as shipping and high-tech industries, resulting in assessments that are theoretical rather than practical. This capacity gap hinders not only preventive measures but also investigation, supervision, and intelligence analysis.

LOW QUALITY SUSPICIOUS ACTIVITY REPORTS/ SUSPICIOUS TRANSACTION REPORTS (SARS/ STRS)

Reports filed by DNFBPs, financial institutions and VASPs often lack detailed narrative, contextual insights, or linkage to predicate proliferation-related offenses. This issue is compounded by poor data quality; Suspicious Transaction Reports (STRs) are often generic and fail to specifically target PF risks. Consequently, authorities are forced to rely heavily on qualitative opinions rather than quantitative hard data, weakening the overall assessment.

Without actionable intelligence in these reports, FIUs struggle to identify genuine proliferation finance suspicions, diminishing the value of the AML / CPF reporting chain.

INSTITUTIONAL FRAGMENTATION AND WEAK CPF GOVERNANCE

Many countries do not yet have a centralized, high-level structure (e.g., national CPF taskforce) responsible for overseeing counter-proliferation finance policy, coordination, and implementation. In the absence of such governance, efforts across sectors are siloed; agencies operate independently, leading to duplication or oversight gaps.

DIPLOMATIC AND POLITICAL CONSTRAINTS

Some Southeast Asian countries maintain historical or strategic ties with jurisdictions subject to non-proliferation sanctions. These ties may dampen political will or delay rigorous CPF engagement. As a result, targeted financial sanctions (TFS) implementation and risk prioritization may be less robust than required, limiting effective disruption.

GEOGRAPHIC AND LOGISTICAL COMPLEXITY

The region's large maritime territories, many small ports, and re-export trade hubs pose monitoring and enforcement challenges. Proliferators may exploit ship-to-ship (STS) transfers or complex routing, which are difficult for customs and enforcement agencies to trace. Furthermore, limited surveillance in certain jurisdictions exacerbates these vulnerabilities.

LACK OF AWARENESS AND TECHNICAL CAPACITY

Proliferation finance remains a niche topic in many domestic AML/CFT regimes. Public and private actors often lack awareness of PF risks, including dual-use goods procurement, front companies, and trade-based schemes. The "need for training programmes" and "enforcement clarity" was emphasized by participants. This points to a notable skills deficit in the region. Training programmes are sparse, and there is insufficient investment in building specialized expertise (e.g., dual-use export control, financial investigation of PF networks).

BENEFICIAL OWNERSHIP OPACITY

Weak corporate registries, reliance on nominee directors, and minimal verification of ownership structures persist in multiple jurisdictions. These conditions make it easier for front companies or shell entities to hide beneficial owners behind proliferation-related financial transactions. Such opacity is a fundamental enabler of proliferation finance in the region.

4.2 Best practices

Despite the many challenges, several Southeast Asian jurisdictions have made notable progress in implementing effective CPF regimes. Drawing on NRAs, mutual evaluation reports, and engagement with the conference working groups, the following best practices emerge:

4.2.1 GOVERNANCE & POLITICAL COMMITMENT

Securing high-level political commitment is crucial. One participant noted a success where the Office of the President issued an order that mandated a whole of government approach to CPF, with the Financial Intelligence Unit (FIU) acting as the main coordinator.

Public–Private Partnerships (PPPs)

Authorities in some countries have engaged proactively with financial institutions, VASPs, shipping firms and registries, and logistics companies to exchange intelligence, raise awareness, and co-develop red-flag indicators.

Utilizing existing AML/CFT (Anti-Money Laundering/Combating the Financing of Terrorism) infrastructure and relationships to advance the CPF agenda, rather than starting from scratch.

Involving academic institutions in the assessment process to broaden the analytical perspective.

4.2.2 INTER-AGENCY COOPERATION

Well-functioning national CPF taskforces, working groups or steering committees have been effectively implemented and utilized in some jurisdictions to facilitate whole-of-government engagement. These structures provide clarity of mandate, coordinate policy development, and ensure alignment across FIUs, customs, export-control bodies, intelligence agencies, and other relevant partners. These set-ups are often developed in close consultation with private-sector actors to ensure practicality, relevance and private-sector buy in.

4.2.3 CAPACITY-BUILDING AND TRAINING INITIATIVES

In partnership with government authorities, region-wide capacity-building programmes, such as thoseconducted by EU P2P, EU Global Facility and the UNODC, have been leveraged to deliver expert-level, train-the-trainer trainings for FIUs, customs, regulators, and anti-financial crime private-sector risk practitioners.

Such initiatives use practical tools, such as scenario-based exercises, red-flag handbooks, and tabletop simulations, to build proficiency in identifying and responding to PF-related risks.

Regional and International Cooperation

Regional Collaboration: Engaging in close cooperation within the region via formal and informal bodies (e.g., FICG) to share information and best practices. Attempting to use real case studies and typologies is being introduced to understand specific sector risks.

EU P2P
Export Control Programme
for Dual-use Goods

CBRN
Centres
of Excellence
An initiative of the European Union

EU AML / CFT
GLOBAL FACILITY

APG
Asia/Pacific Group
on Money Laundering

Part 5: Conclusion

Funded by
the European Union

Part 5: Conclusion

The Southeast Asia Regional Workshop on Proliferation Financing served as a critical diagnostic moment for the region. The findings of the three working groups paint a picture of a region that is economically dynamic and strategically vital, yet systemically vulnerable to exploitation by the world's most sophisticated proliferation networks.

Southeast Asia is confronting a growing and increasingly complex PF threat. While capacity and awareness are expanding, significant challenges remain, ranging from institutional fragmentation and resource constraints to information-sharing bottlenecks and regulatory gaps. At the same time, robust best practice initiatives have emerged, including effective PPPs, targeted guidance, and capacity-building initiatives supported by EU P2P and other providers.

The threats are clear: from the physical smuggling of dual-use components through the region's bustling free trade zones and maritime hubs, to the digital evasion of sanctions via virtual assets and the exploitation of diplomatic channels. The vulnerabilities are equally evident: legislative gaps, data silos, and a lack of specialized enforcement capacity.

The path forward requires a paradigm shift. Southeast Asian jurisdictions must start to view CPF as a core component of national security and economic integrity. By implementing the recommendations and best practices set out in this report—specifically by breaking down inter-agency silos, engaging the private sector as partners, and harmonizing regulations across borders—the region can transform itself from a target of proliferation networks into a bulwark against them.

EU P2P
Export Control Programme
for Dual-use Goods

CBRN
Centres
of Excellence
An initiative of the European Union

eup2p.dug@expertisefrance.fr

EU AML / CFT
GLOBAL FACILITY

www.global-amlcft.eu

EU Global Facility on AML/CFT

APG
Asia/Pacific Group
on Money Laundering

www.apgml.org

APG Secretariat

Funded by
the European Union

This publication was produced with the financial support of the European Union. Its contents are the sole responsibility of the authors and do not necessarily reflect the views of the European Union.