



The International Institute for
Justice and the Rule of Law

Good Practices Manual on Establishing Effective Public-Private Cooperation in Countering the Financing of Terrorism in Southeast Asia



The International Institute for Justice and the Rule of Law

Inspired by the Global Counterterrorism Forum, the IJ was established in 2014 as a centre of excellence providing training and capacity-building for lawmakers, judges, prosecutors, law enforcement and other justice sector practitioners. The institution provides a vital platform to share and promote good practices and sustainable approaches to counterterrorism founded on the rule of law.

The IJ is an intergovernmental organisation based in Malta with an international Governing Board of Administrators representing its **12 members: Algeria, France, Italy, Jordan, Kuwait, Malta, Morocco, Nigeria, Tunisia, Türkiye, the United Kingdom, and the European Union**. The organisation is staffed by a dynamic international team who are responsible for day-to-day operations including practitioner-focused trainings, workshops and research.

Disclaimer

This publication has been produced with the financial support of **Global Affairs Canada**. Its contents are the sole responsibility of the International Institute for Justice and the Rule of Law and do not necessarily reflect the views of Global Affairs Canada.

For more information, please contact:

The International Institute for Justice and the Rule of Law
University of Malta - Valletta Campus
Old University Building, St. Paul Street, Valletta, Malta

info@theijj.org X @ijjmalta theijj.org

Table of Contents

Table of Abbreviations	2
Foreword	4
Executive Summary	5
Introduction	6
Background	7
International Standards	8
Strategic and Operational Information Sharing	9
Strategic Information Sharing	10
Operational Information Sharing	11
Evolution of Information Sharing through PPC	13
Enabling Feedback to the Private Sector	14
Frameworks for PPC	15
Organisational Frameworks	15
Evolutionary and Hybrid Models	19
Legal and Regulatory Challenges and Opportunities	21
Legal and Regulatory Barriers to Public-Private Cooperation	21
Legal and Regulatory Enablers and Good Practices for Public-Private Cooperation	22
Example Legal Frameworks for Cooperation	24
Participation in PPC Mechanisms	26
Vetting, Confidentiality and Ethical Obligations	27
Expanding Membership Beyond Traditional Banking	27
Operational Demands and Response Capabilities	30
Cross-Border Cooperation	31
Financial Inclusion	33
Challenges and Practical Solutions in PPCs for CTF	34
Conclusion	38
Annex 1: Case Studies: Establishing PPC Frameworks for Counter-Terrorist Financing	39
Case Study 1: Australia's FINTEL Alliance - Co-Location Model	39
Case Study 2: Hong Kong's FMLIT - Phased Expansion Approach	42
Case Study 3: Malaysia's MyFINet - Central Bank Leadership Model	44
Annex 2: Enabling Documents (Draft Templates)	46
Draft MoU for Strategic Information Sharing	46
Draft MoU for Operational Information Sharing	47
Tool: PPC Membership Design Checklist (Threat-Led Approach)	49
Further Readings and Resources	50

Table of Abbreviations

ACIP	AML/CFT Industry Partnership
ACIP-CSI	ACIP Case Specific Information
AML	Anti-Money Laundering
AMLC	Anti-Money Laundering Council (Philippines)
ANZ	Australia and New Zealand Banking Group Limited
APG	Asia/Pacific Group on Money Laundering
API	Application Programming Interface
APMG	Association for Project Management Group
AUSTRAC	Australian Transaction Report and Analysis
BIN	State Intelligence Agency or Badan Intelijen Negara (Indonesia)
BNM	Bank Negara Malaysia
BNPT	National Agency for Counter Terrorism or Badan Nasional Penanggulangan Terorisme (Indonesia)
BSP	Bangko Sentral ng Pilipinas
CDD	Customer Due Diligence
COSMIC	Collaborative Sharing of Money Laundering/Terrorism Financing Information & Cases (Singapore)
CTF	Counter Terrorist Financing
DNFBPs	Designated Non-Financial Businesses and Professions
EU	European Union
FATF	Financial Action Task Force
FI	Financial Institution
FINTEL Alliance	Financial Intelligence Alliance (Australia)
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
FIU	Financial Intelligence Unit
FMLIT	Fraud and Money Laundering Intelligence Taskforce (Hong Kong)
GDPR	General Data Protection Regulation
HKMA	Hong Kong Monetary Authority

HSBC	Hongkong and Shanghai Banking Corporation
IMF	International Monetary Fund
IS	Islamic State
Jl	Jemaah Islamiyah
JMLIT	Joint Money Laundering Intelligence Taskforce (United Kingdom)
MACC	Malaysian Anti-Corruption Commission
MLAT	Mutual Legal Assistance Treaty
MoU	Memorandum of Understanding
MSB	Money Service Business
MyFINet	Financial Intelligence Network (Malaysia)
NAB	National Australia Bank
NCA	National Crime Agency (United Kingdom)
NCC	National Coordination Committee (Malaysia)
NGO	Non-Governmental Organisation
NPO	Non-Profit Organisation
ODIN	Operational Danish Intelligence Network
PDPA	Personal Data Protection Act (Malaysia)
PDRM	Royal Malaysia Police or Polis Diraja Malaysia
PPATK	Financial Transaction Reports and Analysis Center or Pusat Pelaporan dan Analisis Transaksi Keuangan (Indonesia)
PPC	Public-Private Cooperation
SIPENDAR	Terrorist Financing Detection and Reporting System or Sistem Pendeteksian dan Pelaporan Dana Terorisme (Indonesia)
STR	Suspicious Transaction Report
TF	Terrorist Financing
UK	United Kingdom
UNSC	United Nations Security Council
UNCTED	UN Counter Terrorism Committee Executive Directorate
VASP	Virtual Asset Service Provider



Foreword

This guide was developed as part of the project, *'Building Capacity and Improving Cooperation Mechanisms on Countering the Financing of Terrorism in Southeast Asia'* funded by Global Affairs Canada.

Cooperation between public and private sectors is a vital component of effective financial investigations that has received increased attention over the last ten years. In part, this is because of the unique challenges that such cooperation presents and innovative mechanisms that many countries have developed to overcome those challenges. Our goal with this publication was to synthesise lessons learned from regional and international public-private cooperation mechanisms into practical guidance for practitioners and policy makers from Southeast Asian countries.

The guide focuses on public cooperation with the financial sector but recognises that entities outside of traditional banking also hold intelligence and evidence relevant to terrorist financing investigations and prosecutions.

Ultimately, we hope that the guide provides a roadmap for jurisdictions to develop and strengthen their respective public-private cooperation mechanisms and compliance with international standards, particularly those set by the Financial Action Task Force.

The guidance is the result of consultations, research and analysis carried out between October 2025 and May 2026. We are deeply grateful to all those who contributed to the development of this guide, particularly those who joined the 'Expert Group Meeting' discussions and consultations. Feedback provided during the drafting process from, among others, APG, UNCTED and private sector stakeholders was essential for development of this guide, as was the valuable contribution of the lead authors and experts, Dr. Jessica Davis and Ms. Munira Mustaffa. Finally, the publication would not have been possible without the generous support of Global Affairs Canada.



Mr. Naoufel Gaied,
Executive Secretary of the IJ

Executive Summary

This publication provides practical guidance for establishing and strengthening public-private cooperation (PPC) to counter terrorist financing (CTF) in Southeast Asia.

The guide addresses PPC within Southeast Asian contexts and focuses on operational and strategic implementation through templates, case studies, and procedural guidance. Notwithstanding its regional focus, international experiences inform recommendations where they can strengthen local practice.

Between October 2025 and April 2026, practitioners from Cambodia, Indonesia, Lao PDR, Malaysia, the Philippines, Thailand and Vietnam contributed insights through surveys, workshops, and consultations to identify effective PPC systems, operational needs, and lessons from diverse regional experiences. This feedback informed the drafting process, while case studies including Australia's FINTEL Alliance, Hong Kong's Fraud and Money Laundering Intelligence Taskforce (FMLIT), and Malaysia's Financial Intelligence Network (MyFINet) were developed to illustrate different approaches to governance and operational coordination.

The Background section establishes regional context by outlining threats and existing capabilities, the guide then defines operational and strategic information sharing, introducing concepts that are given more detailed consideration in subsequent chapters, before examining some common PPC models. Legal and Regulatory Issues identifies barriers to and enablers for information exchange, including confidentiality constraints and statutory protections. Membership addresses participation requirements across diverse entities from traditional banks to fintech platforms and telecommunications providers. The Challenges and Solutions chapter offers practical responses to common obstacles, including technological integration, resource constraints, and cross-border coordination, followed by Opportunities for Partnership, which outlines low-threshold initiatives that could facilitate progress without requiring new legislation or formal agreements. Case Studies examine three frameworks that demonstrate how different jurisdictions approach partnership challenges. Finally, Enabling Documents provides templates and tools supporting implementation, including model agreements and procedural guidance.

This publication is intended for use by competent authorities in designing and establishing PPC frameworks. It is primarily aimed at financial intelligence units (FIUs), law enforcement, and other investigative authorities, as well as their reporting entity partners within the financial sector.

Introduction

Effective CTF efforts depend fundamentally on cooperation between public sector entities (law enforcement, FIU and regulators) and private sector actors (banks, money service businesses, virtual asset service providers, fintech platforms, and other financial intermediaries). Where functional partnerships exist, they enable better understanding of risk, earlier threat detection, more rapid transaction monitoring, and more comprehensive financial intelligence.

Terrorist financing has become harder to detect and disrupt. Legitimate business structures are exploited as fronts for illicit activities.¹ Cryptocurrency mixers and privacy-focused digital assets obscure transaction trails. The convergence of terrorist financing with other forms of illicit finance means that CTF practitioners must now possess expertise across multiple domains to effectively identify and disrupt financial flows.

In recent years, many jurisdictions have developed mechanisms to facilitate cooperation and the efficient, two-way flow of information between public and private sectors. These mechanisms do not replace reporting requirements for regulated entities but enable timely and in-depth exchange of intelligence between institutions. By enabling two-way flow of information, PPC frameworks have been noted to offer significant advantages over relying solely on reporting entities obligations to report suspicious transactions. However, the development of such partnerships across Southeast Asia can be inconsistent.

Practitioners throughout the region identify legal and regulatory constraints on information sharing as the primary obstacle to effective cooperation. Data protection frameworks, while serving legitimate privacy interests, can restrict the timely exchange of information. Cross-border coordination compounds these challenges, as differing legal standards can create friction in regional intelligence sharing. Additional obstacles include insufficient technological integration between public and private systems, misaligned institutional priorities across sectors, and resource constraints that limit both capacity building and operational coordination.

This guidance focuses on PPC in the context of terrorist financing. In most jurisdictions, PPC mechanisms will not be limited to CTF but will also be applied to anti-money laundering (AML) and other types of financial crime and investigations. Nonetheless, specific guidance on PPC in the context of terrorist financing (TF) is important for enhancing capabilities and early detection, filling a critical capacity gap. Globally, the proportion of suspicious transaction reports (STRs) filed in relation to terrorist financing is believed to be low, with money laundering and other financial crime often easier to identify.² Detection and investigation of terrorist financing poses unique challenges, including identification of TF where funds have a legitimate origin such as salaries or charitable donations and use of low-value transactions that go ‘under the radar’ of monitoring and reporting requirements. By concentrating on PPC for CTF, this publication aims to provide practical guidance tailored to the regional needs of Southeast Asia that can address some of these challenges.

The term public-private cooperation is used in this manual in preference to public-private partnerships (PPPs). While PPPs may imply formalised, contractual, or regulatory arrangements, PPC is used here to reflect the broader and more flexible forms of engagement. Cooperation encompasses a spectrum of interactions, from informal information sharing to structured collaborative mechanisms, without presuming a specific legal or institutional form. This distinction is important, as effective CTF collaboration often depends on adaptable, trust-based relationships that extend beyond formal partnership models.

¹ Aryana, Rifana Meika Triskaputri, and Broto Wardoyo Satrya. 2020. "The Dynamics of Funding for the Al-Jama'ah Al-Islamiyah Group." Paper presented at the ICSGS Conference, November 6, 2019.

² Arz El Murr, Terence Donovan and Yee Man Yu. "Chapter 2: The Role of the Private Sector in Detecting and Disrupting Terrorist Financing Activities" in Countering the Financing of Terrorism Good Practices to Enhance Effectiveness. International Monetary Fund, 2023.

Background

The convergence of transnational criminal networks, digital payment systems, and porous borders has transformed terrorist financing across Southeast Asia. This problem demands practical tools that reflect current operational realities.

The terrorist financing landscape has evolved considerably since the Islamic State's (IS's) territorial control period in Iraq and Syria between 2014 and 2017. During that period, supporters in Southeast Asia sustained operations by transporting physical currency across borders and used transfer mechanisms, ranging from conventional banking to informal remittance networks like hawala.³ Individuals traveling to conflict zones typically drew upon their own resources, whether from legitimate sources such as employment income and personal savings or through other means like loans.⁴

The Financial Action Task Force's (FATF) 2025 comprehensive update on terrorist financing risks notes a marked increase in the interlinkage of diverse methods and the integration of digital platforms with traditional methods such as cash transportation and informal value transfer systems.⁵ The proliferation of virtual assets has expanded the toolkit available to threat actors, who have developed capabilities involving cryptocurrency and other digital finance methods. Additionally, the misuse of charitable organisations and informal value transfer systems has complicated efforts to distinguish legitimate financial flows from those supporting terrorist activities.⁶ This evolution creates distinct operational challenges for countering terrorist financing (CTF) and, more specifically, PPC mechanisms.

Meanwhile, the regional security landscape has fragmented, complicating coordinated CTF efforts. For instance, maritime Southeast Asia (Indonesia, Malaysia, Philippines, and Singapore) continues to prioritise terrorism as an urgent threat, while Mekong countries (Cambodia, Lao PDR, Myanmar, Thailand and Vietnam) focus predominantly on cybercrime syndicates, illegal gambling operations, and human trafficking. Countries like the Philippines face overlapping challenges from terrorism financing in conflict-affected areas and transnational organised crimes, including casino-related money laundering.⁷ The emergence of industrial-scale 'scam centres', notably in Cambodia and Myanmar has created spillover effects for other countries in the region, while active armed conflicts in Myanmar add further instability to regional dynamics.⁸

These divergent priorities reflect regional disparities. Southeast Asian jurisdictions operate with varying technological infrastructures and readiness, diverse legal frameworks, and differing institutional capacities.⁹ Some countries possess advanced financial intelligence capabilities, while others are at an early stage in the development of investigative tools and operate with limited interagency coordination. Informal economies remain significant across much of the region, creating parallel financial systems that can evade traditional monitoring mechanisms.

Existing international CTF standards provide an essential baseline for developing domestic CTF frameworks tailored to countries' risk profiles and threat environment.¹⁰ However, practitioners in the region have identified persistent gaps between global frameworks and the practical challenges they confront daily. These include limited resources for financial intelligence analysis, difficulties tracking informal value transfer systems, insufficient mechanisms for PPC and obstacles to timely cross-border information sharing.

³ Lakshmi, Sylvia. "Terrorism Financing in Southeast Asia: Transformations, Continuities and Challenges"; *Counter Terrorist Trends and Analyses*. RSIS, 2022.

⁴ *Ibid.*

⁵ "Comprehensive Update on Terrorist Financing Risks". Financial Action Task Force (FATF), 2025.

⁶ Croissant, Aurel, and Daniel Barlow. "Following the Money Trail: Terrorist Financing and Government Responses in Southeast Asia." *Studies in Conflict & Terrorism* 30 (2), 2007.

⁷ Anti-Money Laundering Council. "Philippines Exits FATF Grey List." Republic of the Philippines, Press release, February 21, 2025.

⁸ Mukherji, Biman. "Can Southeast Asia Contain Growing Threat of Cyber Scams?" *South China Morning Post*, June 6, 2025.

⁹ Sanusi, Zuraidah Binti Mohd, Syahrul Ahmar Bin Ahmad, Sharifah Nazatul Faiza Binti Syed Mustapha Nazri, and Mohammad Aktaruzzaman Khan. "Digital Compliance in Action: A Comparative Study of AML Strategies in Malaysia and Indonesia's Financial Sectors." *International Journal of Academic Research in Business and Social Sciences* 15 (9), 2025.

¹⁰ *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - The FATF Recommendations*; Financial Action Task Force (FATF), updated 2026.

Analysis of Jemaah Islamiyah's (JI) organisational structure between 2019 and 2022 revealed that the group sustained operations through multiple funding streams, including membership dues, 'taxes' from affiliated businesses, networks of madrassas, and charity organisations that collectively raised substantial sums annually.¹¹ Sanctions against JI were first imposed in 2006, targeting its core leadership. Although JI maintained a centralised command structure for much of this period, the arrest of its leader Para Wijayanto in 2019 prompted a deliberate organisational shift towards decentralisation, with local divisions increasingly answering to regional rather than central leadership. This organisational transformation demonstrated the inadequacy of sanctions alone without complementary strategies to disrupt the informal financing mechanisms that decentralised networks rely upon.

International Standards

This manual is grounded in the standards set by the Financial Action Task Force (FATF). While no single recommendation governs PPC, many FATF provisions collectively require and support the exchange of information. Moreover, the value of such cooperation mechanisms has been recognised in mutual evaluations.

The following Recommendations collectively establish the legal, institutional, and operational foundations for information sharing, feedback, and coordinated action between public authorities and the private sector:

- Recommendation 1, Risk-Based Approach
- Recommendation 2, National Cooperation and Coordination
- Recommendation 20, Suspicious Transaction Reporting
- Recommendation 29, Financial Intelligence Units
- Recommendation 31, Powers of Law Enforcement and Investigative Authorities
- Recommendation 34, Guidance and Feedback

PPCs also directly contribute to the achievement of key effectiveness outcomes under the FATF methodology, particularly:

- Immediate Outcome 1, Risk Understanding and Coordination
- Immediate Outcome 6, Financial Intelligence
- Immediate Outcome 9, Terrorist Financing Investigation and Prosecution
- Immediate Outcome 10, Targeted Financial Sanctions

It follows that PPC is foundational to both technical compliance and the effective functioning of national AML/CTF systems.

United Nations Security Council Resolution 2462 (2019) *"encourages competent national authorities, in particular financial intelligence units and intelligence services, to continue to establish effective partnerships with the private sector, including financial institutions, the Financial technology industry and internet and social media companies, in particular with regards to the evolution of trends, sources and methods of the financing of terrorism"*.

¹¹ Satria, Alif; "Understanding Jemaah Islamiyah's Organisational Resilience (2019-2022)." International Centre for Counter-Terrorism (ICCT), 2023.

Strategic and Operational Information Sharing

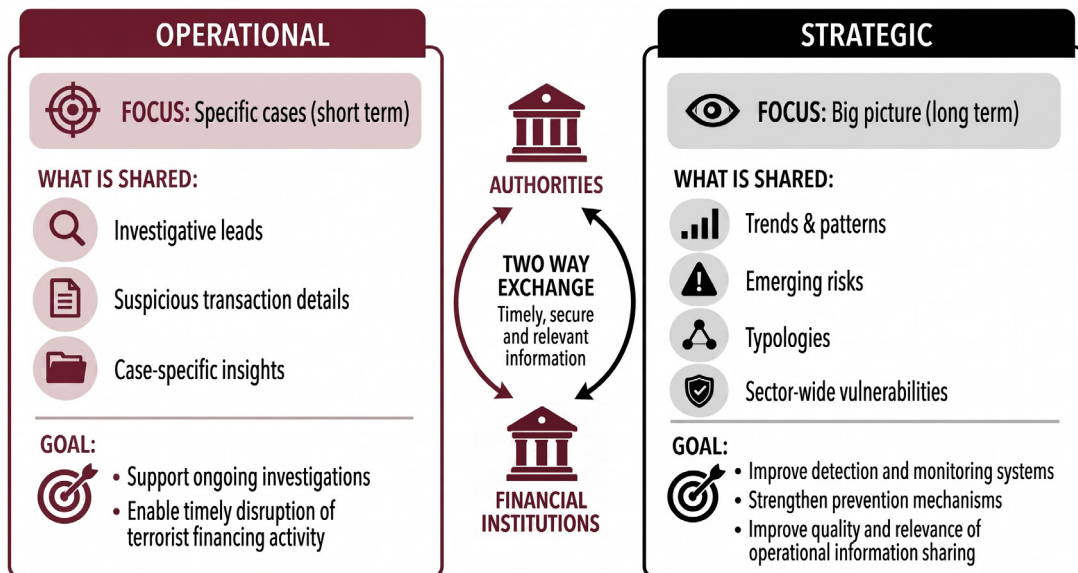


Figure 1: Strategic and Operational Information Sharing

PPC models in CTF are generally structured around two complementary but distinct forms of collaboration: operational and strategic information sharing. Together, these form the foundation of effective collaboration in identifying and disrupting terrorist financing activity.

- **Operational (tactical) information sharing** focuses on the exchange of tactical intelligence, such as investigative leads, suspicious transaction details, and case-specific insights, between authorities and financial institutions to identify new intelligence, support ongoing investigations and enable timely disruption of terrorist financing activity.
- **Strategic information sharing** by contrast, involves the sharing of broader analytical insights, including trends, emerging risks, typologies, and sector-wide vulnerabilities. These strategic exchanges help institutions and authorities better understand evolving terrorist financing methods and strengthen detection and prevention mechanisms, ultimately improving the quality and relevance of operational information sharing.

While mutually reinforcing, the information typologies have distinct requirements in terms of governance structures, technological platforms, information-sharing protocols, and legal frameworks governing data protection, confidentiality, and permissible use of financial intelligence.

Strategic Information Sharing

Strategic information-sharing provides a platform for financial institutions and competent authorities to deepen their collective understanding of evolving terrorist financing threats. Unlike operational information sharing, which focuses on immediate investigations or case-based exchanges, strategic information sharing supports longer-horizon analysis, the identification of macro-level patterns, and the refinement of collective threat assessments. This enables a risk-based approach by supporting improved understanding of the threat environment and development of proportionate measures in response. The core purpose of strategic information sharing is to help both sectors anticipate misuse of the financial system to enable them to adapt and strengthen prevention and detection.

Core Analytical Activities

Strategic information sharing typically begins with the synthesis of reporting streams, most often suspicious transaction reports (STRs) and transaction reports. By aggregating these inputs, analysts can refine their understanding of the threat landscape and identify recurring behaviours or emerging anomalies, often resulting in operational alerts, typologies, or indicators.

Studies on typologies and trends play a central role: they examine patterns over defined periods, track how methodologies evolve, and surface new operational leads before they are widely recognised in the system.¹² Because terrorist groups and other illicit actors continuously adapt to regulatory and enforcement pressure, this type of analysis must be ongoing.

Several forms of strategic analysis can be undertaken within PPC mechanisms.

- **Group-, movement-, or ideology-based analyses** examine how specific entities raise, move, store, manage, use and hide funds, drawing on multiple information types to understand their financial ecosystems.
- **Attack-financing analysis** looks at the financial characteristics of individual incidents.
- **Attack-financing profile pattern analysis** aggregates multiple events to identify commonalities across ideologies, geographies, or actor types, including lone-actor events.
- **Indicator development** is another key activity, ensuring that early-warning signs are observable, measurable, and refined through testing.

Strategic analysis can also focus on countries or sectors to highlight vulnerabilities linked to jurisdictions, areas of territorial control, or industry structures. These country- and sector-specific assessments help identify financial channels that facilitate the movement of funds and can support both strategic and operational analyses.

Another strength is flexibility: strategic information sharing can adapt to focus on emerging themes, new methodologies, or system-wide vulnerabilities. Because it generally relies on aggregated or anonymised information, insights can be shared that are less sensitive than operational data, lowering barriers to participation. Therefore, strategic information sharing can involve multiple partners, such as through regional or thematic sessions, or function bilaterally when a narrower scope is required.

Strategic information sharing creates a virtuous cycle in which high-level analysis feeds into improved detection, which in turn supports operational follow-up.¹³ Even when operational and strategic exchanges occur separately, interoperability between PPC mechanisms strengthens threat-mitigation efforts.

Strategic information sharing also helps build trust and relationships between institutions, often laying the groundwork for deeper case-based operational cooperation over time.

¹² For example, see Canada's [Project Anton](#).

¹³ Based on feedback provided following the EGM.

Challenges and Considerations

Notwithstanding its value, focusing only on strategic information limits the utility of PPCs. High-level analysis can be difficult to translate into operational leads without additional mechanisms for tactical follow-up. Cross-jurisdictional differences in reporting regimes, sectoral structures, and terrorist financing risk profiles can also complicate the interpretation of shared typologies or patterns; “crosswalks” are often required to ensure that insights generated in one jurisdiction can be meaningfully applied in another.

Finally, if information-sharing efforts stop at the strategic level, the PPC might not achieve its full potential. Strategic PPCs should be viewed as a gateway to more operational forms of collaboration, rather than a standalone solution.

Illustrative Models

Several existing initiatives demonstrate the value of strategic information-sharing frameworks.

The AUSTRAC Fintel Alliance includes a strategic component that shares indicators, typologies,¹⁴ and STR-derived insights on issues such as child exploitation and terrorist financing.¹⁵ Similarly, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) produces operational alerts that support strategic information sharing by Canadian PPC mechanisms such as Project Anton and Project Protect. Singapore’s COSMIC platform (an example of private-to-private cooperation) enables banks to identify emerging financial crime patterns by sharing red-flag indicators related to suspicious clients, typologies, and network behaviours across institutions.¹⁶ Malaysia’s MyFINet supports system-wide awareness by disseminating emerging typologies—including trade-based money laundering, mule-account networks, and fintech-enabled fraud—across banks and authorities.¹⁷ Malaysia’s 2025 Mutual Evaluation Report highlights how systematic intelligence sharing through MyFINet, “helps raise awareness amongst FIs and, in some cases, leads to additional disclosures or STR filings for authorities to analyse”.¹⁸

These models illustrate how strategic PPCs can strengthen upstream detection and create the conditions for more effective operational collaboration.

Operational Information Sharing

Operational (or tactical) information sharing tends to be shorter-term and case specific. The objective is to improve detection, investigation and disruption through mechanisms that enable efficient exchange of information and gathering of evidence, often in response to emerging cases that present a high degree of urgency. PPC in this context facilitates exchange of information beyond formal reporting requirements and more efficiently than via multiple bilateral relationships.

From the perspective of the private sector, participation in operational PPC mechanisms enables a better understanding of the threat from criminal actors, which leads to improved risk management, minimising the likelihood of terrorist financing exposure and consequent legal and reputational liabilities. Participation in operational PPC mechanisms can also enable a higher level of feedback to the private sector on the value of information provided.

¹⁴ “Discover purpose behind the Fintel Alliance”. Australian Transaction Reports and Analysis Centre (AUSTRAC)

¹⁵ “Fintel Alliance – Child Exploitation Indicators,” AUSTRAC. “Terrorist Financing Risk Assessment Guidance”; FATF, 2019.

¹⁶ Fenengo, “MAS Launches COSMIC Platform for KYC Data Sharing”; Fenengo, 2024.

¹⁷ Marzunisham, Omar; “Welcoming remarks by Mr Marzunisham Omar, Deputy Governor of the Central Bank of Malaysia (Bank Negara Malaysia), at the 23rd Asia/Pacific Group on Money Laundering (APG) Typologies Workshop”, 9 November 2021. “Malaysia National Risk Assessment On Money Laundering and Terrorism Financing 2023”.

¹⁸ “Mutual Evaluation of Malaysia”; APG, 2025.

Core Analytical Activities

Three core areas of operational cooperation can be identified:¹⁹

- i. Identification of new investigative leads
- ii. Evidence gathering for ongoing cases
- iii. Disruption of identified threats

Within these areas, PPC mechanisms can support the development of investigations in multiple ways including identification of new leads during ongoing investigations or at the conclusion of an investigation, monitoring, locating and/or linking suspects through financial activities and identification of assets for asset recovery. Operational information sharing mechanisms thereby contribute to effective investigation and prosecution of terrorist financing.²⁰ Mechanisms may also support exchange of information between private institutions. Finally, by sharing intelligence that enables the private sector to better understand what is requested and why, and by providing timely feedback regarding the utility of information, PPC mechanisms strengthen long-term engagement and the overall quality of reporting.

Challenges and Considerations

The main challenges associated with operational information sharing relate to the sharing of highly confidential information. Operational information sharing will likely require competent authorities to share details of an investigation and private sector institutions to share personal data. It is important that such information sharing has a clear legal basis, that PPC mechanisms are not used to circumvent legislative safeguards, and that information sharing remains proportionate and necessary, including application of data minimisation principles.²¹

Due to the sensitivity of operational information sharing, members of PPC mechanisms may require vetting to enable them to access classified or sensitive information with consequent implications for the size and structure of PPC mechanisms.

While engagement can offer multiple advantages for private sector entities, it is also recognised that participation is often resource intensive and may be challenging for smaller entities, particularly those without dedicated compliance units.²² This is especially the case where mechanisms require attendance at regular meetings or even secondment. It is important that participation does not come at the expense of other reporting requirements and that mechanisms strive to enable participation of a diverse range of private sector entities, not only large financial institutions for whom participation may be relatively easy in relation to available resources.

Other challenges include the need for adequate resources including dedicated staff within the competent authority, meeting space and technological platforms that can enable the efficient and secure exchange of information.

Illustrative Models

Recent years have seen an increase in countries adopting operational PPC models. One of the first countries to develop mechanisms for operational information sharing was the United Kingdom through the Joint Money Laundering Intelligence Taskforce (JMLIT).²³ Since then, multiple jurisdictions have developed operational information sharing mechanisms including Australia (Fintel Alliance), Singapore (ACIP), and Hong Kong (FMLIT).

¹⁹ "EFIPPP Practical Guide for Operational Cooperation between Investigative Authorities and Financial Institutions"; Europol, 2025.

²⁰ FATF Immediate Outcome 9: Terrorist financing offences and activities are investigated and persons who finance terrorism are prosecuted and subject to effective, proportionate and dissuasive sanctions.

²¹ Fn. 19

²² See: Aidoo, Samuel, "Evaluating the Effectiveness of Public-Private Partnerships in Anti-Money Laundering: U.S. Case Studies, Global Insights, and Policy Implications" 2025.

²³ In its 2018 Mutual Evaluation of the United Kingdom FATF observed JMLIT to be an 'example of best practice' contributing to the effectiveness of CTF frameworks.

Evolution of Information Sharing through PPC

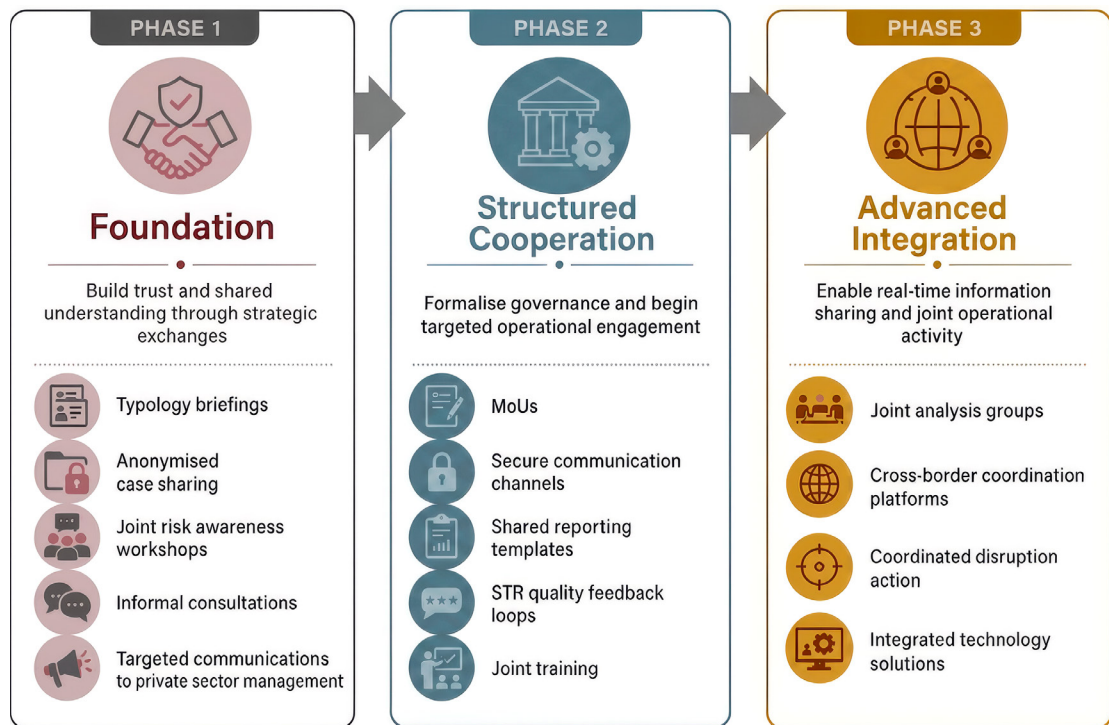


Figure 2: Evolution of Information Sharing through PPC

A useful way to conceptualise the evolution of PPCs in CTF is through a maturity framework that reflects increasing levels of trust, capability, and operational integration.

In many jurisdictions, PPCs begin with foundational strategic information sharing, where participants exchange high-level insights on risks, trends, and typologies. This phase allows partners to establish governance structures, clarify legal boundaries, and build the trust necessary for more sensitive collaboration. As the partnership matures, PPCs often transition to more advanced operational models, incorporating the exchange of case-specific information, coordinated analysis, and, in some instances, near-real-time collaboration to support active investigations. At higher levels of maturity, PPCs may enable joint analytical workflows, rapid feedback loops on suspicious transaction reporting, and proactive identification of targets or networks. While this progression is neither linear nor universal, the movement from strategic to increasingly operational engagement reflects a shift toward greater impact in detecting and disrupting terrorist financing activity, supported by more robust legal frameworks, technological infrastructure, and institutional relationships.

There is no 'one size fits all' model for PPC. Different jurisdictions face different risk profiles and have differing resources and developmental levels. In most jurisdictions, PPC frameworks will evolve as systems develop and adapt to meet the risk profile, needs and capacity of the respective jurisdictions.

Even at foundational levels, PPC can strengthen understanding of risk, detection and prevention contributing to more effective CFT systems.

Enabling Feedback to the Private Sector

A consistent concern raised by the private sector is the lack of feedback received from law enforcement/FIUs in response to STRs. Reporting entities invest considerable resources in transaction monitoring and report preparation. Without information on whether those reports contribute to investigations, disruptions, or prosecutions, the relationship can become one-directional, and over time, compliance culture might weaken as entities question whether their reports are being read, acted upon, or producing any outcome. Moreover, the absence of feedback directly affects report quality. Compliance officers who receive no indication of how previous reports were used have a limited basis for improving subsequent submissions or identifying corrective measures.²⁴ The International Monetary Fund (IMF) has identified feedback to reporting entities as a core mechanism for improving both the flow and quality of STRs.²⁵ Without structured feedback to close the loop or help private entities feel engaged, reporting risks becoming a compliance checkbox rather than a substantive intelligence contribution.

By facilitating a two-way dialogue between public and private sectors, PPC mechanisms can provide a forum for enabling more in-depth feedback on private sector reporting. This can include competent authorities providing more detail on information requests and providing insights into the operational utility of information provided (subject to limitations on sharing sensitive information, particularly in the context of ongoing investigations) – or simply giving the private sector a better understanding of the realities of operations that may take months or even years to reach a conclusion. Through dialogue mutual trust, understanding and engagement can be enhanced.

Some jurisdictions have formalised feedback processes through MOUs between FIUs and LEAs that include explicit obligations, creating accountability on both sides of the relationship. In Cambodia's experience, for example, signing an MOU with law enforcement helped establish frameworks for sharing intelligence reports, including feedback mechanisms requiring law enforcement to evaluate intelligence quality.²⁶

²⁴ Fn. 2

²⁵ IMF, "[Financial Intelligence Units: An Overview](#)"; International Monetary Fund, 2004 and *Ibid.*

²⁶ International Institute for Justice and the Rule of Law (IJJ), Expert Group Meeting on Public-Private Partnerships for Countering Terrorist Financing in Southeast Asia, April 2025.

Frameworks for PPC

This section examines model frameworks for PPC and considers how PPCs function in practice across Southeast Asia, drawing on experiences from Cambodia, Indonesia, Lao PDR, Malaysia, the Philippines, and Thailand.

Common features of effective PPC models include:

- i. organisational frameworks that structure coordination and sustain engagement.
- ii. information sharing mechanisms that enable intelligence exchange.
- iii. operational workflows governing suspicious transaction reporting and rapid response; and
- iv. technological infrastructure supporting the exchange of information.

Jurisdictions operate at different maturity levels, from those establishing frameworks to those refining advanced systems, while identifying practical challenges encountered in implementation.

Organisational Frameworks

PPCs employ different structural approaches to coordinate information exchange and operational collaboration. Three primary models can be identified:

- i. hub-and-spoke models centralising coordination through a single entity.
- ii. integrated database platforms enabling distributed access; and
- iii. multi-pillar frameworks dividing functions across specialised structures.

Each model creates different information flow patterns, decision-making processes, resource and coordination requirements.

i. Hub-and-Spoke Models

Hub-and-spoke models operate by routing all information through a central coordinating entity that manages both inbound intelligence and outbound dissemination.

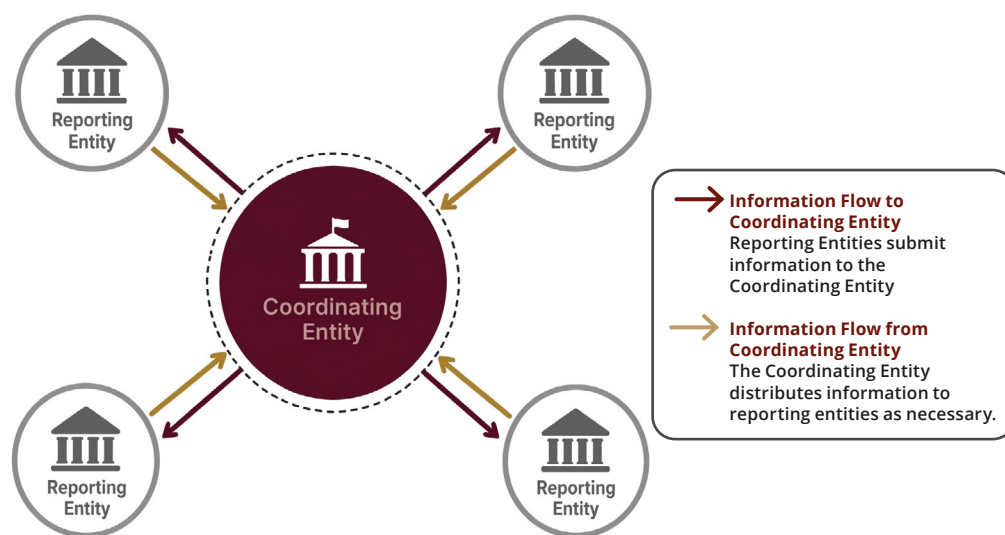


Figure 3: Hub and Spoke Model

The United Kingdom's Joint Money Laundering Intelligence Taskforce (JMLIT) provides a good illustration of how these models can operate.

The National Crime Agency (NCA) serves as the hub. Information sharing is enabled through primary legislation that permits any entity or individual to share information with the NCA,²⁷ provided it is for the exercise of NCA functions.²⁸ This means that financial institutions sharing information with the NCA do not breach banking secrecy or data protection regulations so long as information is shared for a legitimate purpose. The NCA can also share information with public and private sector entities – in the exercise of its functions. In this way, the NCA acts as a gatekeeper (hub) that facilitates information sharing across a range of public and private entities.

JMLIT operates two parallel tracks:

- i. an operational component that handles case-specific intelligence for active investigations; and
- ii. thematic working groups that generate strategic threat analyses.

The NCA coordinates regular meetings in which law enforcement agencies discuss investigative requirements with participating financial institutions. These institutions represent approximately 89 per cent of UK personal account volume, providing substantial coverage while maintaining manageable coordination through the central hub (NCA).²⁹ In the ten years since its establishment in 2015, JMLIT supported approximately 1,200 operations, 419 arrests, over 250 million GBP in asset restraint, and identified thousands of accounts previously unknown to investigators.³⁰ The model demonstrates how centralised routing reduces the complexity that would arise from multiple bilateral relationships between individual banks and law enforcement agencies.

²⁷ Section 7, Crime and Courts Act 2013

²⁸ Functions of the NCA include gathering, analysing and disseminating information to combat crime (including organised and serious crime). Section 1, *Ibid.*

²⁹ Fn. 23

³⁰ "10 Years of Public Private Partnerships Against Economic Crime", SARs in Action Magazine, NECC PPP Team, 2025.

According to FATF “[t]he UK proactively investigates, prosecutes and convicts a range of TF activity, in line with its identified risks in this area. A particularly positive feature of the system is the strong public/private partnership on TF matters. This is facilitated by the Joint Money Laundering Intelligence Task Force (JMLIT) which facilitates public/private information sharing including on TF and ML investigations.”³¹

Other examples of hub and spoke models include Singapore’s AML/CFT Industry Partnership (ACIP). ACIP facilitates both operational, case specific, information sharing through ‘hub and spoke’ model taskforces and strategic information sharing through publication of ‘Best Practice Papers’.³² In its 2026 Mutual Evaluation report, FATF observed:

“Singapore also has a public private partnership, the ACIP, which brings together nine materially significant banks with all relevant competent authorities in Singapore. This venue facilitates open discussion on actual cases and trends [...]. ACIP also creates ACIP Case-Specific Information (ACIP CSI) taskforces to detect and develop priority cases. Through these taskforces, tactical information is shared with members through a hub-and-spoke model, which conduct further analytics on their information holdings to surface new leads. Such sharing has resulted in positive outcomes, as well as enhancements in the relevant FIs’ risk understanding which in turn leads to better risk mitigation and AML/CFT controls. These taskforces are also used to co-ordinate actions during major investigations. These ACIP-CSI taskforces go beyond the membership of the nine permanent FI members to other FIs, VASPs and DNFBPs, as needed. There was positive feedback from ACIP members and government authorities indicating that the ACIP was leading to real world results.”³³

Other examples of ‘hub and spoke’ models for PPC include Hong Kong’s Fraud and Money Laundering Intelligence Taskforce (FMLIT) and Denmark’s Operational Danish Intelligence Network (ODIN).

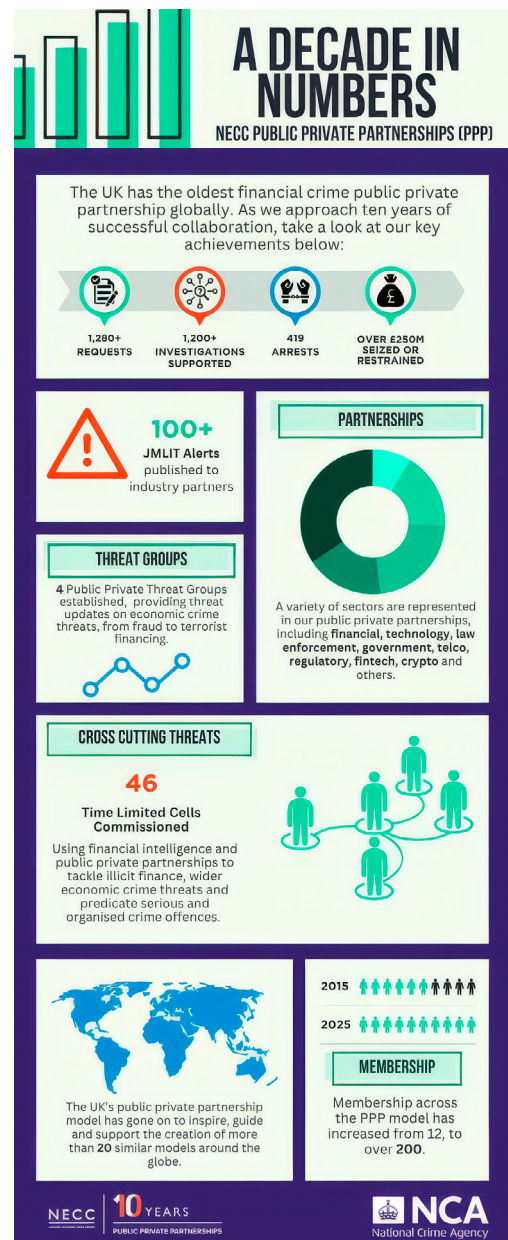


Figure 4: A Decade in Numbers; source National Crime Agency (https://www.linkedin.com/posts/celebrating-10-years-of-the-uks-public-private-share-7349434384690606082-5001/?utm_source=share&utm_medium=member_desktop&rcm=ACoAADbj6wBA8BDYA-2pvqgQgnHyhiufkC8hMA)

³¹ United Kingdom Mutual Evaluation Report; FATF, December 2018. <https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-united-kingdom-2018.html>

³² “AML/CFT Industry Partnership (ACIP)”, Monetary Authority of Singapore

³³ Para 152. *Mutual Evaluation of Singapore*; APG, May 2026.

ii. Integrated Database Model

Integrated database models facilitate the exchange of information and enable multiple authorities to access shared intelligence repositories through tiered access controls.

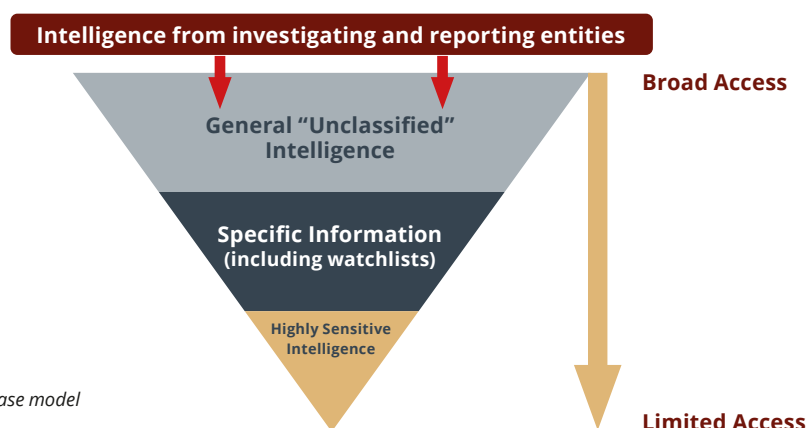


Figure 5: Integrated database model

Indonesia's SIPENDAR system demonstrates this approach by connecting the FIU with investigating agencies and a high number of private sector reporting entities through a three-tier information structure. General, non-classified, terrorism financing information circulates at the broadest level of access and is regularly updated. This information includes sanctions listings, national and sectoral risk assessments, watch lists and typologies.³⁴ Private sector entities are expected to monitor the platform for information, including 'watchlists' issued by PPATK, and report relevant information through SIPENDAR, such as exposure to monitored individuals/entities.

Highly sensitive source material is limited to designated personnel in intelligence and investigative agencies. Prior to accessing the system, other users must pass vetting and background checks by the competent authorities. Thereafter, users authenticate through the system, which determines levels of access based on pre-authorised roles while logging all queries for audit purposes.

Competent authorities including PPATK, Detachment 88 (Indonesian National Police), State Intelligence Agency (Badan Intelijen Negara or BIN), National Agency for Counter Terrorism (Badan Nasional Penanggulangan Terorisme or BNPT), DG Customs and Excise and DG Immigration, can submit spontaneous information and requests for information through the platform enabling efficient dissemination of requests, which supports effective investigation and prosecution. In case of terrorism incidents or when the request is made for immediate response, private sector entities are required to provide information within 24-hours. Dissemination of sanctions designations and watchlists and consequent increased monitoring has been found to support disruption of TF. This architecture enables simultaneous access by multiple parties without requiring information to route through a single coordination point. However, it also demands robust technical infrastructure and clear access governance protocols.

Sanctions & PPC: CTF sanctions arise from United Nations Security Council measures, as well as bilateral, multilateral, and autonomous (national) regimes. The adoption and implementation of sanctions beyond UN obligations are sovereign decisions, and national approaches vary.

PPCs focused on CTF prioritise terrorism-related sanctions, particularly those targeting designated individuals, entities, and networks. Within this context, PPCs can support the prevention, identification and investigation of sanctions evasion by disseminating designation lists, enabling the exchange of typologies, indicators, and operational insights, and by strengthening coordination between public authorities and the private sector – thereby contributing to the effectiveness of these preventative measures.³⁵

³⁴ Paras 223 and 224, [Indonesia Mutual Evaluation Report](#); FATF, 2023.

³⁵ See for example, the Indonesian SIPENDAR mechanism. FATF's effectiveness indicator, Immediate Outcome 10: 'Terrorists, terrorist organisations and terrorist financiers are prevented from raising, moving and using funds', provides additional guidance on standards of implementation that may be expected here. [Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT/CPF Systems](#); FATF, 2022 (updated 2026).

iii. Multi-pillar Framework

Multi-pillar frameworks distribute operational functions across specialised structures operating in parallel.

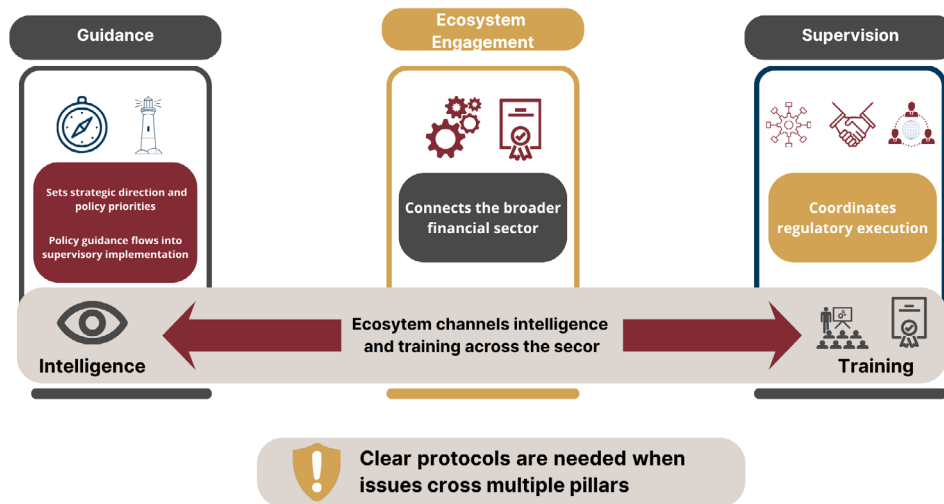


Figure 6: Thailand PPC Model

Thailand's AML/CTF cooperation employs three distinct pillars: policy guidance establishing strategic direction, joint supervision coordinating regulatory implementation, and ecosystem development engaging the broader financial sector. Each pillar manages specific coordination functions while maintaining communication channels with other pillars. Policy decisions flow from the guidance pillar to implementation through the supervision pillar, while ecosystem engagement disseminates intelligence and training across the sector. This division enables specialisation while requiring clear protocols governing how information and decisions transfer between pillars, particularly when issues span multiple operational areas.

Evolutionary and Hybrid Models

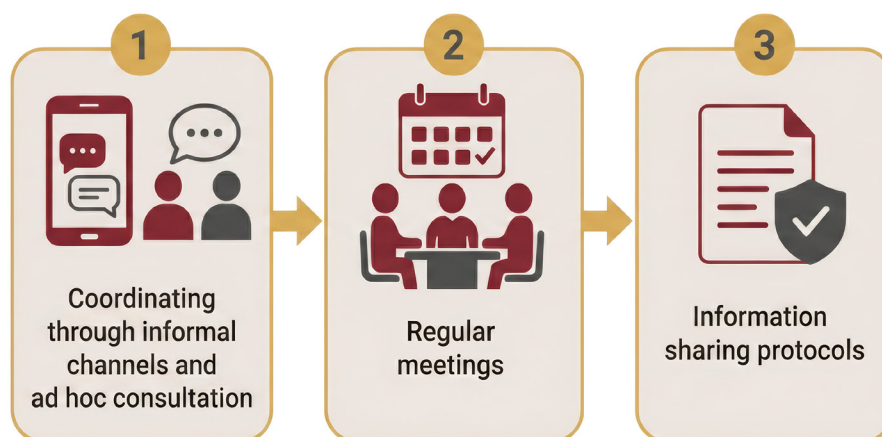


Figure 7: Evolutionary Models

Additional to the three most common frameworks, some jurisdictions combine elements from different frameworks to create models adapted to their own context and resources. These are best described as evolutionary or hybrid models. Evolutionary models develop partnerships through phased progression from informal engagement to structured frameworks.

Cambodia illustrates this evolutionary approach: initially coordinating through informal channels, including messaging applications and ad hoc consultations, before establishing regular quarterly workshops and eventually formalising information-sharing protocols. This staged development enables jurisdictions with limited resources to demonstrate partnership value through low-threshold initiatives whilst building institutional capacity and trust necessary for more structured cooperation. The model recognises that immediate implementation of sophisticated architectures may prove unachievable for jurisdictions at early maturity stages, providing realistic pathways for progressive development.

Other PPC models include hybrid models combining elements of two or more of the primary models or combinations of formal and informal structures.

The Philippine approach builds on traditional reporting requirements through coordination platforms and enhanced focus on sectors assessed as high risk. The Philippine National Police (PNP) and Anti-Money Laundering Council (AMLC, Philippine FIU) work together to synthesise information from other government agencies, including the Department of Justice. The AMLC provides a bridge to the private sector to facilitate information exchange as required. In addition, intensive bilateral work is undertaken between government agencies and private sectors assessed as high risk. Information from these bilateral engagements is fed back to the PNP and AMLC, as required. Meanwhile, the National AML/CTF/PF Coordinating Committee (NACC) functions as the central policy making body and provides centralised, policy-level support for PPC initiatives

These diverse approaches demonstrate that no single model dominates practice. Structural choices reflect legal frameworks that enable information sharing, institutional capacity that supports coordination demands, and operational maturity that shapes implementation feasibility.

These architectures illustrate how partnerships succeed when structures align with available resources, legal authorities, market characteristics, and threat landscapes.

Effective partnerships share common operational features: clear information-routing protocols, defined decision authority, and mechanisms for both routine coordination and rapid escalation, regardless of architectural choice.

Legal and Regulatory Challenges and Opportunities

Legal and Regulatory Barriers to Public-Private Cooperation

Across Southeast Asia, a range of legal and regulatory constraints continue to shape how PPCs operate in CTF. While PPC mechanisms have developed significantly in recent years, uncertainty over data-governance frameworks continue to restrict timely, risk-focused information sharing. The following key barriers illustrate how gaps in legal authority, outdated restrictions, and insufficient safeguards can undermine confidence and inhibit effective collaboration.

- 1. Limited Statutory Mandates for Formal PPC Mechanisms:** Many forms of PPC in Southeast Asia exist informally rather than through established legal or regulatory frameworks. Where PPC forums, task forces, or advisory groups are not supported through legislation or binding regulations, participation can be inconsistent and dependent on goodwill rather than institutional commitments. This reduces continuity and sustainability.
- 2. Fragmented or Ambiguous AML/CTF Legal Frameworks:** In several jurisdictions across Southeast Asia, the legal basis for information sharing is distributed across multiple acts, regulations, and policies, often with limited clarity about which types of information may be shared, by whom, and for what purposes. This ambiguity creates uncertainty among reporting entities and even regulators, discouraging proactive engagement for fear of breaching legal or regulatory obligations. As a result, information sharing tends to be conservative, limited, and largely reactive.
- 3. Lack of Standardised Safeguards for Sensitive Information:** In many PPC contexts, legal and procedural frameworks governing the secure handling, access controls, proportionality, or auditing of shared information remain underdeveloped or completely absent. Without standardised safeguards, both public and private partners face exposure to cyber risk, legal challenge, or political scrutiny. These are conditions that can erode trust and limit willingness to engage in information sharing. These gaps carry broader implications as well, such as absence of formalised agreements with accountability mechanisms, PPC arrangements become vulnerable to legitimate criticism of human rights and privacy grounds, thus undermining public confidence that CTF frameworks ultimately depends on.
- 4. Legacy Bank Secrecy and Confidentiality Laws:** Strong and sometimes outdated bank secrecy laws continue to restrict the ability of financial institutions to share risk-relevant information with peers or even with law enforcement outside of STRs. While these laws were initially designed to protect consumer confidentiality and financial stability, they can inhibit legitimate sharing for CTF purposes, slowing down operational responses to emerging threats.³⁶
- 5. Absence of Legal Protections for Good-Faith Sharing:** In some jurisdictions, there is no explicit legal protection or indemnity for financial institutions that share information or intelligence in good faith but later prove to be incorrect or incomplete. Without such protections, institutions face the risk of civil litigation, regulatory penalties, or reputational damage. This creates a strong disincentive to participate in PPCs, especially when terrorist financing cases can be ambiguous, fast-moving, or evolving.

³⁶ This persists even though FATF Recommendation 9 states that financial secrecy provisions must not inhibit implementation of its recommendations, i.e., FATF standards should take precedence over financial secrecy.

- 6. Over-Reliance on STR-Centric Information Flows:** AML/CTF systems in much of the region remain designed primarily around one-directional reporting: from financial institutions to the FIU, rather than two-way intelligence or information exchange. This limits opportunities for risk dialogue, typology sharing, or joint analysis. It also reinforces a compliance-oriented mindset rather than one grounded in shared security outcomes.
- 7. Constraints on Cross-Border Information Sharing:** Terrorist financing in Southeast Asia is inherently transnational, yet data protection rules, secrecy laws, and jurisdictional restrictions often limit the transfer of financial intelligence across borders. Even when exchange is permitted, the legal processes required may be lengthy or complex, reducing timeliness and operational utility, particularly in rapidly evolving threat environments.

Taken together, these barriers highlight that legal uncertainty and restrictive frameworks remain among the most significant obstacles to effective PPC in the region. Where laws do not clearly enable proportionate, secure, and purpose-driven information exchange, institutions tend to default to conservative, compliance-focused behaviour. Addressing these regulatory constraints through clarified mandates, legal protections, and standardised safeguards will be critical to unlocking the full potential of PPC CTF efforts across Southeast Asia.

Legal and Regulatory Enablers and Good Practices for Public–Private Cooperation

Despite the barriers, there are significant opportunities to strengthen PPC through legal, regulatory, and policy enablers that provide clarity, certainty, and trust. The following measures illustrate how proportionate legal authority, privacy safeguards, and structured governance can create a secure foundation for meaningful information sharing to counter terrorist financing.

- 1. Clear Legal Authority for Information Sharing:** Public-private cooperation is strongest where the legal framework explicitly permits FIUs, law enforcement, and reporting entities to exchange risk-relevant information for AML/CTF purposes. When legislation clearly defines what may be shared, under what conditions, and with whom, institutions gain the confidence needed to engage fully in partnership activity. Legal certainty reduces the perceived risk of liability, enables more proactive collaboration, and helps shift institutional behaviour from defensive compliance toward joint problem-solving. Absent or pending legislative changes, competent authorities can identify information-sharing that is permitted and develop PPCs accordingly. Even PPCs focused on strategic information sharing can strengthen CFT effectiveness and support establishment of operational mechanisms when the legal/regulatory framework is established.
 - 2. Legal Protections for Good-Faith Reporting and Sharing:** Several jurisdictions have introduced statutory protections or indemnities for financial institutions that share information or file reports in good faith. These protections reduce the risk of civil or administrative action where suspicions later prove unfounded. Such measures enable open dialogue between public and private actors and can foster a culture of collaboration rather than legal risk-avoidance.
 - 3. Formal Recognition of Public–Private Cooperation Mechanisms:** When PPC forums, working groups, or task forces are recognised or mandated in legislation, regulation, or policy announcements, participation becomes institutionalised rather than personality-driven. Formal mandates help ensure continuity, dedicated resourcing, and clearer governance structures. They also create a legitimate channel for consultation and two-way intelligence exchange, elevating PPC from an informal activity to a core feature of the AML/CTF system.
 - 4. Privacy-by-Design Safeguards in Legal and Regulatory Frameworks:** Public confidence and institutional trust are strengthened when legislation requires strong governance, access controls, proportionality tests, data-minimisation practices, and audit trails for information sharing. Embedding these safeguards in the regulatory framework rather than leaving them voluntary or ambiguous, establishes a predictable and secure environment that reassures both industry and regulators while supporting operational cooperation.
-

Case Study Good Faith Protections: Singapore

Singapore has developed two statutory safe harbour provisions that enable information sharing:

- i. The Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) protects persons who make disclosures in good faith from civil liability and from any claim that the disclosure breached a legal, contractual or professional obligation.³⁷
- ii. The Terrorism (Suppression of Financing) Act ("TSofA") provides a comparable protection specifically for terrorism financing, shielding persons who disclose information in good faith from civil and criminal proceedings that may arise from those actions.³⁸

Coupled with these protections, in 2018, Singapore strengthened its enforcement framework following concerns that existing penalties were insufficient to deter non-compliance.³⁹ A case that year illustrated the problem: a property agent was fined for failing to file a STR after learning that his client was linked to a major foreign Ponzi scheme, with the court noting that the then-maximum fine of \$20,000 was too low to function as a meaningful deterrent.⁴⁰ The 2018 amendments raised maximum penalties substantially and expanded Singapore's ability to exchange financial intelligence with foreign FIUs.

5. **Clear Standards on Data Retention, Deletion, and Onward Use:** Clarity around how long data may be retained, for what purpose, and under what conditions it may be shared onward reduces uncertainty for PPC participants. These rules help ensure proportionality while still permitting meaningful operational use.
6. **Common Baseline Standards for Regional Data Sharing:** Given the transnational nature of terrorist financing in Southeast Asia, regional alignment of data-sharing standards is a key enabler. Developing common baseline privacy and data-protection requirements would ensure that a minimum standard is consistently applied across jurisdictions.⁴¹ This approach would facilitate cross-border information flows, reduce legal uncertainty for multinational institutions, and create a foundation for regional cooperation while respecting national sovereignty.
7. **Structured Information-Sharing Agreements and MoUs:** Formal agreements, whether bilateral or multilateral, provide legal clarity on purpose limitation, retention rules, governance, and security controls. These instruments help operationalise cooperation in a way that is both legally compliant and practically workable. They also create accountability and transparency, strengthening trust between sectors and across borders.
8. **Independent Oversight and Accountability Mechanisms:** Oversight by courts, parliaments, data-protection authorities, or other independent bodies creates legitimacy for PPC and helps ensure that cooperation remains lawful, proportionate, accountable and aligned with democratic values. Transparent oversight frameworks increase public trust, making PPC more sustainable over the long term while protecting human rights.

Together, these enablers reflect the importance of legal clarity, standardised protections, and credible oversight for effective PPC. Where these elements are in place and aligned across the region, institutions are more willing and able to collaborate, resulting in a more effective response to terrorist financing.⁴²

³⁷ Singapore, Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A), Section 39(6).

³⁸ Singapore, Terrorism (Suppression of Financing) Act (Cap. 325), Section 8.

³⁹ Mei, Tan Tam, "Parliament: Harsher Penalties for Terrorism Financing, Money Laundering and Money Mules," *Straits Times*, 2018.

⁴⁰ "Former Real Estate Agent Fined \$10,000 for Failing to Flag Suspicious Deal" *Straits Times*, 2018.

⁴¹ For example, the EU General Data Protection Regulation (GDPR), which establishes common data protection standards across the European Union.

⁴² Immediate Outcomes 6 (financial intelligence), 9 (prosecution and investigation of TF) and 10 (preventative measures).

Example Legal Frameworks for Cooperation

The private sector is bound by data protection and other privacy laws. Specific legal pathways enable sharing of information while respecting data protection safeguards, providing reassurance for the private sector and ensuring legitimacy and engagement. When PPC frameworks are expanded beyond the traditional financial sector, legal pathways enabling cooperation need to address legal obligations specific to those sectors to ensure that barriers to participation are adequately met.⁴³

Three jurisdictions illustrate different approaches to addressing these challenges.

Indonesia

Indonesia's legal framework demonstrates how jurisdictions can work with existing bank secrecy provisions to enable broader participation. Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering and Law No. 9 of 2013 on the Prevention and Eradication of Terrorism Financing grants the Pusat Pelaporan dan Analisis Transaksi Keuangan or PPATK (PPATK/Financial Transaction Reports and Analysis Centre), Indonesia's FIU, authority to access financial institution information notwithstanding bank confidentiality laws.⁴⁴

The law establishes suspicious transaction reporting requirements and provides PPATK with authority to postpone transactions. Importantly, the law also protects reporting entities from liability for good faith reporting.⁴⁵ This statutory provision removes institutional uncertainty about legal consequences, creating an explicit exception for AML/CFT purposes while maintaining confidentiality protections.

Customer Due Diligence (CDD) regulations also allow private-private information sharing within a defined financial group, or more broadly when required to address a specific purpose (e.g. to tackle mass fraud/scam centres).

Thailand

Thailand demonstrates how privacy concerns can constrain cooperation even when legal authority exists. The Anti-Money Laundering Act (1999) establishes the legal basis for private sector cooperation in detecting and reporting terrorist financing activities.⁴⁶ Thailand's Personal Data Protection Act (PDPA) (2022) exempts AML/CTF operations from its scope and therefore should not limit reporting. Nonetheless, financial institutions remain concerned about privacy violations despite this clear statutory authority. This hesitation demonstrates how uncertainty about data protection boundaries and risk-averse interpretations can complicate cooperation.

United Kingdom

The UK's PPC framework relies on two elements: a legislative gateway that enables information sharing and an operational mechanism that puts it into practice. Key to this regime is the role of the NCA as an intelligence hub and gatekeeper for information sharing. The function of the NCA is defined as gathering, storing, processing, analysing, and disseminating information to combat crime and recover the proceeds of crime.

⁴³ For example, data protection rules applied to telecommunication providers are likely to be different to those applied to financial industries. See: [Chadderton, Paula, and Simon Norton, "Public-Private Partnerships to Disrupt Financial Crime: An Exploratory Study of Australia's Fintel Alliance."](#) SWIFT Institute Working Paper No. 2017-003, 2019.

⁴⁴ Article 28, [Law Number 8 Year 2010 Concerning the Prevention and Eradication of the Crime of Money Laundering](#).

⁴⁵ Article 29, *Ibid* states: "Unless there is an element of power abuse, no civil suits or criminal charges can be filed against a Reporting Party, official, and his/her employees for implementing the reporting obligations in accordance with this Law".

⁴⁶ Thailand. ["Anti-Money Laundering Act B.E. 2542 \(1999\)."](#)

Section 7, Crime and Courts Act 2013, creates the provisions that enable information sharing for PPC. These include:

- i. Information can be shared with the NCA for the exercise of NCA functions
- ii. The NCA can share information obtained in connection with its function provided the disclosure is for a permitted purpose (this includes sharing with other government bodies and international partners)
- iii. Sharing information with the NCA under Section 7 does not breach confidentiality or other restrictions on disclosure of the information.

These provisions enable two-way information sharing while protecting participants from liability. The onus is placed on the NCA to analyse, sanitise and share received information appropriately and in accordance with its function.

Case Study Building Partnerships from Early Stages: The Lao PDR Experience*

The experience of Lao PDR illustrates addressing challenges in building public-private partnerships. The country has a strong AML/CFT legal framework, designated authorities with clear mandates, and a willingness amongst regulators and private actors to collaborate. However, critical gaps remain as there is not a clear legal provision for two-way information that meets data protection concerns. Beyond formal reporting requirements, private sector engagement remains limited to informal, ad-hoc information exchanges.

Lao PDR has adopted a four-step model to address these challenges.

Step 1: focuses on legal foundations, conducting gap analysis between existing frameworks and FATF standards, whilst examining cooperation models from other jurisdictions.

Step 2: establishes dialogue platforms that bring together the FIU, financial institutions, and sectoral regulators to build relationships and mutual understanding.

Step 3: implements pilot strategic information-sharing focused on specific typologies, allowing participants to understand value while building trust and confidence in controlled circumstances.

Step 4: formalises successful pilots into permanent frameworks, scaling what works and adjusting what does not.

This phased approach recognises that effective partnerships require more than legal authority. Lao PDR has adopted a system that allows both sectors to demonstrate how cooperation operates in practice before committing to permanent arrangements. This progression from informal engagement through structured pilots to permanent frameworks provides a realistic pathway for jurisdictions at early stages of partnership development.

**As reported during an IJJ workshop in April 2025*

Participation in PPC Mechanisms

PPC participation will depend on multiple factors including national and sectoral risk profiles, resource constraints, vetting requirements, developmental level and capacity. At early stages in development, competent authorities might opt to limit engagement to reporting entities and/or high-risk sector/s and subsequently expand engagement based on necessity.

Layered Engagement Example

One model for PPC participation can be conceptualised as a set of layered engagements, with a consistent core and flexible outer components that adapt to jurisdictional needs and threat contexts. At its core, PPCs typically include law enforcement (including police services), financial intelligence units (FIUs), and other investigative or competent authorities, alongside financial institutions and reporting entities, including those operating in emerging financial and technological sectors.

Beyond this core, PPCs can incorporate additional participants on a contextual or needs basis. This might include actors from the non-profit sector, often engaged through representative or umbrella bodies, as well as technology and communications stakeholders such as social media platforms, internet service providers (ISPs), and sectoral initiatives or consortia (e.g., GIFCT, Tech Against Terrorism). These participants can provide valuable contextual, technical, or network-level insights that complement financial intelligence.

This layered approach allows PPCs to maintain a stable operational foundation while expanding or contracting participation as required, ensuring that the right actors are engaged to address specific risks, typologies, or investigative priorities without overextending governance or information-sharing frameworks.

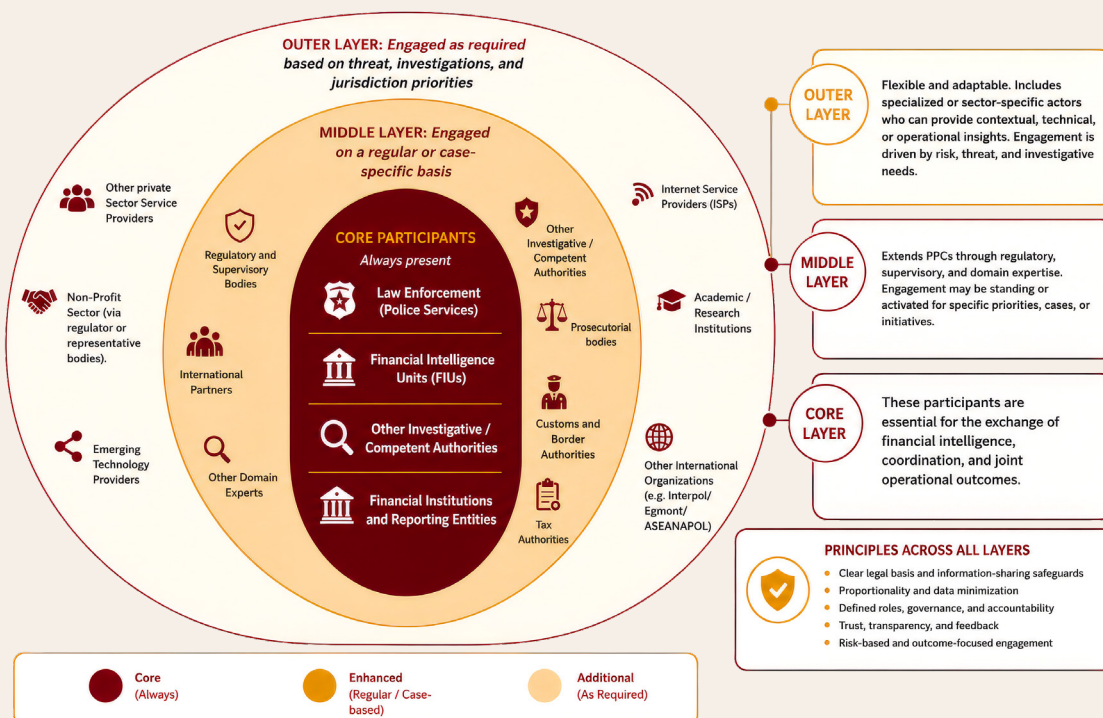


Figure 8: Layered PPC Participation Model

Vetting, Confidentiality and Ethical Obligations

Access to sensitive intelligence requires vetting procedures that match personnel clearance levels to the sensitivity of the information. Strategic cooperation involving sanitised typology reports and aggregated trend analysis imposes minimal vetting requirements, whereas operational collaborations involving case-specific intelligence require background checks and security clearances.

Confidentiality protocols and public safety require balancing information sharing with protection obligations through access controls, ensuring participants receive only information appropriate to their roles and clearance levels.

For example, the UK's JMLIT and Denmark's ODIN engage vetted private sector representatives with appropriate clearances for handling law enforcement intelligence, while Indonesia's FIU maintains capacity for urgent responses through analysts who receive advance clearance rather than emergency vetting during a crisis.

Expanding Membership Beyond Traditional Banking

Virtual Asset Service Providers

FATF's 2019 update brought VASPs within AML/CFT requirements, but jurisdictions soon discovered that implementation challenges extend beyond traditional financial sector supervision.⁴⁷ Meaningful risk assessments require understanding blockchain technology, mixing services, privacy coins, and decentralised finance protocols. Effective legislation requires the ability to distinguish between VASP categories, as exchanges that convert crypto to fiat operate differently from peer-to-peer platforms or decentralised autonomous organisations. Building competent authorities requires technical capacity that few jurisdictions possess, particularly in blockchain analysis and virtual asset tracing.

The Philippines has developed one of the strongest VASP frameworks in the region outside Singapore. VASPs must register with the Bangko Sentral ng Pilipinas (BSP) or the Securities and Exchange Commission, depending on their activities. They face the same reporting obligations as other covered persons.⁴⁸ As of December 2025, approximately 19 VASPs held BSP licences, mostly operating as remittance agents or crypto-to-fiat exchanges. Although no specific VASP legislation exists yet, the framework provided through regulatory memorandum gives sufficient authority for supervisory oversight and for integrating reporting.

Under Indonesia's CFT framework the independent Financial Services Authority (OJK / Otoritas Jasa Keuangan) is primarily responsible for Indonesia's virtual asset regulatory framework. The agency's mandate includes licensing and registration, AML/CFT compliance oversight, sectoral risk assessment, on-site inspection, and formulating travel rule protocols for virtual asset transfer among traders.⁴⁹

⁴⁷ "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" FATF, 2021.

⁴⁸ Bangko Sentral ng Pilipinas, "Guidelines for Virtual Asset Service Providers (VASP)"; Office of the Governor, Circular No. 1108, 2021.

⁴⁹ Fn. 34

Fintech Platforms and Digital Payment Systems

Fintech platforms and digital payment systems serve populations that conventional banking often does not reach, including undocumented foreign workers, asylum seekers and refugees.⁵⁰ E-wallets and mobile payment systems like Touch 'n Go and GrabPay have become increasingly ubiquitous across much of Southeast Asia, with adoption outpacing cash and card payments in several major regional economies.⁵¹ The same accessibility that drives financial inclusion, however, creates channels that operate outside conventional AML/CFT oversight frameworks. Many fintech firms were not originally designed with AML/CFT compliance infrastructure in mind, and the regulatory frameworks governing them vary significantly across the region. Some jurisdictions have moved to address this. For example, Malaysia's MyFINet incorporates fintech providers and electronic money operators as full participants in its intelligence-sharing framework, and Australia's FINTEL alliance has expanded membership to include remittance providers and digital currency exchanges.

As the payments landscape continues to shift towards digital channels, leaving these firms outside intelligence-sharing frameworks means an increasingly large portion of the financial system operates without meaningful oversight or integration.

Money Services Businesses

Money services businesses (MSBs), including remittance providers, currency exchanges, and informal value transfer systems, occupy a critical position in terrorist financing ecosystems.

In 2016, a JAD member used a well-known global MSB for remittance to purchase weapons for a planned attack, which was eventually thwarted.⁵²

Telecommunications, Social Media and Other Non-Financial Providers

Telecommunications providers present different considerations. Thailand and Cambodia have identified these providers as critical partners on the basis that terrorist financing requires communication, and those communications generate data that can reveal network structures, planning timelines, and financial arrangements.⁵³ However, telecommunications data contains extraordinarily sensitive information, and partnership structures must be carefully designed. **The objective should be to enable targeted, intelligence-led queries, not dragnet surveillance that violates privacy principles and produces overwhelming volumes of irrelevant data. The same logic extends to internet service providers (ISPs) and social media platforms, which are increasingly relevant given their use for fundraising, recruitment, and coordination.**

The proliferation of dedicated fundraising platforms and social media has introduced new regulatory risks. Platforms such as GoFundMe, and social media channels including X, have been used for fundraising in ways that are faster than traditional channels. Recipients sometimes request payment in virtual assets, adding a further layer of opacity. Many of these crowdfunding campaigns fall below the thresholds that trigger formal terrorism or illicit financing reporting obligations. Despite ongoing efforts to strengthen trust and safety capabilities across the sector, platforms continue to face challenges in preventing and detecting the abuse of their services for terrorism financing purposes.⁵⁴ Jurisdictions need to develop a clearer picture of how these channels are being used, identify which platforms present the highest risk, and work toward proportionate responses that do not stifle legitimate fundraising.

⁵⁰ Morgan, Peter and Huang, Bihong, "Fintech in ASEAN+3 and Implications for Financial Inclusion and Financial Stability," in Redefining Strategic Routes to Financial Resilience in ASEAN+3, ed. Diwa Guinigundo et al. Asian Development Bank, 2022.

⁵¹ "Now top of mind, cashless could be top of wallets in the near future"; Visa/CLEAR, 2024.

⁵² Soeriaatmadja, Wahyudi. "Trial of Terrorist in Jakarta Sheds Light on Arms Trail from Southern Philippines to Indonesia." Straits Times, 2018.

⁵³ Cambodia Mutual Evaluation Report. Asia Pacific Group on Money Laundering, 2017

⁵⁴ Crowdfunding for Terrorism Financing; FATF, 2023.

An effective PPC framework might also consider engagement with actors in the unregulated or less-regulated sectors, such as travel agents and other service providers. For instance, social media companies can add significant value by providing contextual and network-level information such as user associations, communication patterns, and campaign dynamics, which complements financial data. While fundraising activity might occur on these platforms, the reporting entities are typically payment processors; however, social media platforms themselves can help illuminate the surrounding ecosystem and relationships behind financial flows.

While these entities typically fall outside formal AML/CTF obligations and are not required to participate in PPC mechanisms, their voluntary inclusion (or inclusion of their representative bodies) can enhance situational awareness and provide valuable leads.

Any non-reporting entity participation in PPCs should be carefully structured, clearly voluntary, and supported by appropriate legal safeguards, guidance, and trust-building measures to ensure clarity around roles, expectations, and permissible information sharing.

Non-Profit Organisations

Consideration might also be given to the non-profit sector. Terrorist actors exploit charities and non-profit organisations (NPOs) in varied and often nuanced ways, ranging from fully complicit front organisations to cases where individuals in positions of control divert funds or resources without broader organisational awareness. Beyond fundraising, charities can facilitate the movement of funds across jurisdictions and provide cover, legitimacy, or access for terrorist networks, though such abuse remains relatively limited and highly context-dependent within the broader financing landscape.⁵⁵

While direct participation by individual NPOs in PPCs might be sensitive and, in some contexts, difficult to operationalise, NPO regulators play an important role as intermediaries, holding oversight perspectives and sector-specific risk insights. The inclusion of regulators in PPC mechanisms might therefore be considered appropriate in some circumstances. Umbrella organisations representing NPOs could also be considered for inclusion, providing a more practical entry point for engagement, enabling information sharing at a sectoral level without placing undue burden or risk on individual organisations.

Engagement with the NPO sector should remain voluntary, proportionate, and supported by clear safeguards to maintain trust and avoid unintended chilling effects on legitimate activities.

⁵⁵ Davis, Jessica, "Illicit Money: Financing Terrorism in the Twenty-First Century"; Lynne Rienner Publishers, Inc., 2021.

Operational Demands and Response Capabilities

Expanding partnerships to include fintech platforms, telecommunications providers, and MSBs requires sustained capacity building beyond initial onboarding. These entities often lack the established AML/CFT compliance cultures that major banks have developed over decades. Three jurisdictions demonstrate different approaches to building and maintaining capacity across diverse participants.

Cambodia

Cambodia's experience demonstrates what the capacity gap looks like in practice when partnerships expand beyond major banks. When Cambodia's FIU (CAFIU) began actively engaging non-traditional reporting entities, annual STR volumes were fewer than ten. The problem was not unwillingness but the absence of compliance infrastructure and institutional knowledge of larger banks. Addressing this required sustained, differentiated engagement over several years, through regular shared learning sessions, direct outreach to individual institutions, accessible communication channels, and feedback mechanisms that showed smaller entities the operational value of reporting. The increase in STRs that followed was not the result of any single intervention. It was the cumulative product of treating non-traditional partners as requiring ongoing development rather than one-time onboarding.⁵⁶

Indonesia

Indonesia's approach involves continuous training on terrorist financing indicators, network analysis, and suspicious transaction reporting. This model recognises that initial training becomes insufficient as threats evolve and addresses that through continuous training.

Training is tailored in recognition that fintech startups, telecommunications providers, and smaller money services businesses require sustained support that major banks with dedicated compliance departments may not need.

Thailand

Thailand emphasises that the effectiveness of PPC mechanisms relies not only on systems and regulations. Partnerships are fundamentally 'people driven'. Regular seminars, workshops, training programmes, and coordination meetings create sustained engagement. Sharing typologies and emerging trends keeps participants up to date, while regulatory updates ensure mutual understanding of obligations and operational challenges. Newer participants benefit from relationship building that formal structures alone cannot provide.

⁵⁶ International Institute for Justice and the Rule of Law (IJR), Expert Group Meeting on Public-Private Partnerships for Countering Terrorist Financing in Southeast Asia, April 2026. See also [Cambodia Financial Intelligence Unit, Annual Report 2024](#); CAFIU, 2024.

Cross-Border Cooperation

Legal frameworks and data protection regimes vary considerably between jurisdictions. These variations create compliance challenges for partnerships seeking to establish cross-border information protocols.⁵⁷ Individual entities may also be reluctant to share information that may be used by international counterparts for fear of falling foul of differing legal standards outside their respective jurisdictions.

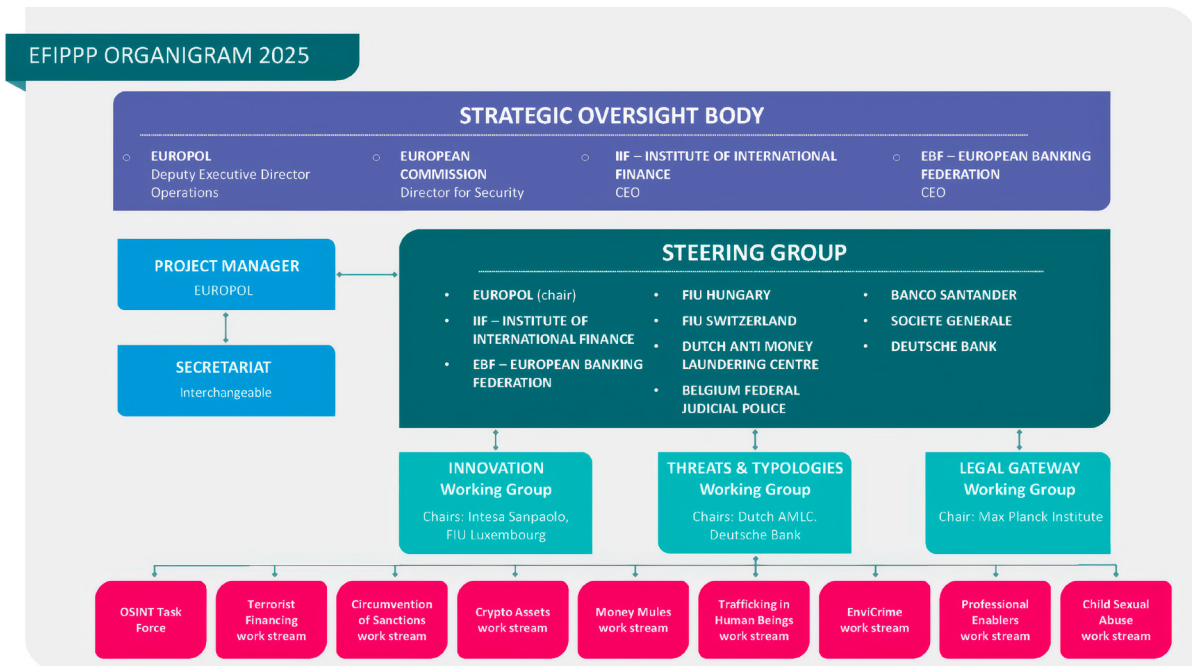


Figure 9: EFIPP Organigram 2025. Source <https://efipp.eu/>

While these challenges have meant that most PPC mechanisms operate only at the national level, there are examples of PPCs facilitating cross-border information. The U.K.'s JMLIT allows international partners to submit requests for information to the mechanism and the governing legal framework permits sharing of information by the NCA with foreign counterparts for defined purposes. Consequently, FATF have noted that a "particularly strong feature of the system is the public/private information sharing through JMLIT to which foreign counterparts may submit requests for consideration".⁵⁸

The Europol Financial Intelligence Public Private Partnership (EFIPPP) provides an example of a regional PPC mechanism. Established in 2017, the mechanism facilitates the exchange of information between Europol, competent authorities including FIUs and law enforcement, and private sector entities.⁵⁹ As of 2025, EFIPPP included 96 representatives from 27 European Union (E.U.) and non-EU countries,⁶⁰ supporting exchange of both operational (tactical) and strategic intelligence across sectors and jurisdictions.

⁵⁷ Medina, Ayman Falak. "Navigating Data Protection Laws in ASEAN-6: A Guide for Foreign Investors." ASEAN Briefing, 2024.

⁵⁸ United Kingdom Mutual Evaluation Report, FATF 2018.

⁵⁹ Further information available at: <https://efipp.eu/>

⁶⁰ Europol Financial Intelligence Public Private Partnership 2024 Annual Report (Public Version); August, 2025.

Within Southeast Asia, ASEAN plays a central role in regional security cooperation. The ASEAN Convention on Counter Terrorism (ACCT) and Treaty on Mutual Legal Assistance in Criminal Matters (MLA Treaty) are two of the legal instruments called for under the Vientiane Action Programme (VAP) to facilitate and harmonise cooperation between ASEAN law enforcement and judicial agencies. Enacted in 2007, the ACCT provides the closest regional approximation of a CTF mandate: Article VI commits parties to preventing and suppressing the financing of terrorist acts and to exchange information as an early warning mechanism.⁶¹

As UN member states, ASEAN countries are also bound by UNSCR1373 (2001), which provides the broader international cooperative framework for countering terrorism.⁶² One of the earliest regional commitments to CTF came from the ASEAN Regional Forum (ARF), which issued a dedicated statement against terrorism financing as early as 2002, committing participating states to implement UNSCR1373, freezing terrorist assets, and enhancing information sharing across the region.⁶³ In 2017, East Asia Summit leaders adopted a dedicated statement on AML and CTF, reaffirming the region's commitment to disrupting terrorist financing networks.⁶⁴ Despite these frameworks, ASEAN member states, like many countries internationally, remain hindered by a tendency to work in silos. Practitioners and policymakers across the region have consistently identified this as a problem, including during Malaysia's 2025 Chairmanship.⁶⁵

Siloing is often reinforced by geographical separation between agencies, different departmental priorities that can override broader CTF goals and legal constraints that can restrict information sharing across jurisdictions. Over time and if unchecked, these barriers may become embedded in institutional culture, thus producing a default disposition against sharing information or intelligence beyond one's own agency. This is compounded by a structural gap at the regional level. ASEAN's primary mechanism for counter-terrorism cooperation is the Senior Officials Meeting on Transnational Crime (SOMTC), which serves as the lead sectoral body for cross-sectoral and cross-pillar cooperation against terrorism and transnational crime.⁶⁶ Within this structure, counterterrorism and money laundering are each addressed through dedicated Working Groups, but there is no equivalent mechanism for CTF specifically. ASEAN recently established a dedicated Working Group on Money Laundering in 2025. A hoped-for progress would be an equivalent mechanism for CTF, which sits at the intersection of counterterrorism and financial crime.

A key recommendation that emerged from the Expert Group Meetings was to leverage ASEAN as a platform for a dedicated CTF information sharing channel for the region. Rather than duplicating existing mechanisms such as the Asia/Pacific Group on Money Laundering (APG) or FATF-style bodies to which many ASEAN member states already belong, a dedicated ASEAN CTF coordination channel may serve as a regional operationalization layer, translating global standards into context-specific cooperation among member states.

⁶¹ Article VI, [ASEAN Convention on Counter Terrorism](#)

⁶² Hafidz, Tatik S. "[A Long Row to Hoe: A Critical Assessment of ASEAN Cooperation on Counter-Terrorism](#)." *Kyoto Review of Southeast Asia* 11, 2009.

⁶³ "[ARF Statement on Measures Against Terrorist Financing](#)" ASEAN Regional Forum, 2002.

⁶⁴ "[East Asia Summit Leaders' Declaration on Anti-Money Laundering and Countering the Financing of Terrorism](#)," 2017.

⁶⁵ Bernama. "[Malaysia Calls for ASEAN to Stop Working in Silos for Regional Peace, Stability and Growth](#)." *Malay Mail*, 2025.

⁶⁶ "[ASEAN Senior Officials Meeting on Transnational Crime \(SOMTC\)](#)." ASEAN Secretariat, 2023.

Financial Inclusion

PPC mechanisms should examine whether counter-terrorist financing measures create indirect discrimination through differential effects on financial access across population groups. Measures should be proportionate to demonstrated threats while avoiding blanket exclusions that marginalise populations without security justification.

Financial institutions are required to apply due diligence and refrain from entering transactions where there is a risk that funds are linked to criminal activity. Information shared through PPC mechanisms may bring unintended consequence of financial institutions refusing to provide services to customers to avoid potential liability (so-called, “de-risking”),⁶⁷ which has been associated with financial exclusion for individuals or groups of individuals.

EFIPPP observes, “[i]n principle, information shared by investigative authorities should not cause adverse consequences. Such consequences should only be permissible if financial institutions, through their own analysis of customer data or through additional sources, establish objective grounds that indicate criminal misuse of their services”.⁶⁸

Trainings and joint briefings offer an opportunity to underline the importance of evaluating transactions based on objective operational characteristics and that decisions must never be based on personal attributes such as gender, race, religious affiliation, or national origin.

Gender: The United Nations Security Council (UNSC) adopted Resolutions 2242 and 2617 in 2015 and 2021, respectively, requiring gender integration across counter-terrorism activities and recognizing that measures perceived as neutral can produce unintended gendered impacts. Financial institutions applying broad risk categories sometimes disproportionately exclude women-led charitable organisations, treating smaller and newer entities as inherently suspicious regardless of operational legitimacy. Women experiencing limited formal banking access in certain contexts face vulnerability, as financial exclusion can push legitimate transactions into unregulated channels.

⁶⁷ Dolan, Carl and Bergin, Jamie, “Public-private partnerships for financial information sharing”; U4 HELPDESK ANSWER, 2025.

⁶⁸ Fn. 19

Challenges and Practical Solutions in PPCs for CTF

Effective public-private cooperation for CTF must address operational, legal, technological, and cultural barriers. These challenges determine whether cooperation succeeds in identifying, disrupting, and preventing terrorist financing or stalls due to uncertainty, under-resourcing, and institutional mistrust. Survey evidence from practitioners across Southeast Asia confirms that the following challenges are among the highest priorities facing regional CTF frameworks.

This section analyses the most pressing challenges and presents practical solutions drawn from regional experience in Cambodia, Indonesia, Lao PDR, Malaysia, the Philippines, and Thailand, alongside established models from outside the region.

1. Technological Integration Between Sectors and Across Borders

Public and private sector institutions across the region operate fragmented, non-interoperable systems with varying data standards, formats, and security protocols. This creates:

- delays in accessing financial intelligence.
- inconsistent data structures and quality.
- duplication of reporting.
- reliance on manual or ad-hoc communication.

Even when systems exist, reporting entities might have differing technical capacities, notably the case for smaller financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs).

When technology is fragmented, quality and efficiency suffer. In the context of CTF, this has real consequences for public safety and security.

Practical Solutions

- i. In the shorter term, agreement on a standardised format and method for sharing financial data, including through the development of templates to standardise reporting and communication. These should be combined with secure email systems and standard encrypted messaging tools for sharing information securely.
 - ii. Development of a unified, interoperable, secure platform that provides a single point of access, enables real-time Application Programme Interface (API) -driven alerts, creates a dashboard for case feedback, and structures communication would address these challenges more effectively in the longer term.
-

2. Joint Investigations and Operational Coordination Across Borders

Terrorist financing networks rarely operate within a single jurisdiction. Yet legal standards, evidentiary thresholds, designation procedures, and banking confidentiality laws differ significantly across Southeast Asia and beyond. Even where cooperation is strong and evidence compelling, designation and enforcement outcomes may diverge or stall.

Operational obstacles include:

- different standards for terrorist designation.
- inconsistent authority to suspend or freeze assets.
- reliance on MLAT or court processes.
- bank secrecy limitations.
- differing priorities or political considerations.

These create operational impacts such as delays in freezing funds, parallel but unaligned actions that undermine disruption efforts, and investigations that conclude without reciprocal outcomes.

Practical Solutions

Use FIUs as trusted bridges between counter-terrorism investigations, utilising support of the Egmont Group when appropriate. This would build on successful models such as Indonesia's SIPENDAR, AUSTRAC's joint-analysis models and Operational Alerts produced under Canadian models such as Project Anton.⁶⁹ While primarily intended for domestic use, such analyses can be used to support the work of international counterparts. The following tools can facilitate joint investigations:

- i. Create joint analysis working groups: These working groups are characterised by recurring secure meetings, shared intelligence briefs, a structured workplan, and multilateral and multisectoral participation.
- ii. Develop legal framework crosswalks: Create short aide-memoires of differences across jurisdictions between freezing authorities, designation standards, reporting thresholds, privacy constraints, and legal definitions of terrorist financing.
- iii. Develop escalation pathways: In CTF, an investigation can rapidly escalate to an immediate threat-to-life investigation. Preparing for this eventuality will enable immediate action. In each PPC, create a light-touch process or point of contact for immediate escalation.

3. TF Typologies and Risk-Based Approach

Terrorist financing takes many forms in the region, from high-value, low-volume transactions to high-volume, low-value transactions, as well as self-funding of terrorist activity and broader support for terrorist organisations from identity-based support networks. This poses challenges for rules-based detection systems (rules and algorithms within financial institutions) and makes reliance on single-institution data a poor approach, as transactions and networks span both institutions and jurisdictions. Further diversifying the terrorist financing environment is a shift to virtual assets, micro-transaction patterns, the integration of fraud and cyber-enabled crime, and the abuse of humanitarian/charitable /NGO/NPO channels.

These dynamics reinforce the importance of adopting a risk-based approach to CTF, in which authorities and financial institutions allocate resources and controls proportionate to the risks they face. In this context, risk assessments that incorporate the terrorist threat, emerging methods, sectoral vulnerabilities, and evolving typologies are essential to ensure that detection, monitoring, and mitigation measures remain targeted, adaptive, and effective.

⁶⁹ For example: [Project Anton](#)

Practical Solutions

While no organisation, institution or jurisdiction has solved these issues, some good practices can facilitate better detection and identification of terrorist financing targets:

- i. Develop scenarios to replace simple indicators: Simple red-flag indicators often miss terrorist financing realities. Scenario-based analysis instead examines full behavioural patterns — including networks, timing, purpose, and geography — to identify plausible terrorist financing pathways. This approach improves detection accuracy, reduces false positives, and aligns much more closely with how terrorist financing occurs in Southeast Asia.
- ii. Maintain situational awareness of the threat environment through strategic intelligence PPCs: Public-private partnerships should not focus only on compliance reporting, but also on strategic intelligence sharing about evolving threats, typologies, and regional dynamics. Regular intelligence exchanges, briefings, and collaborative analysis help institutions anticipate rather than simply react to terrorist financing risks. This continuous situational awareness allows faster operational response and supports proportionate, risk-based decision-making across both sectors.

4. Limited Resources and Capacity Constraints

Many FIUs, regulators, and reporting entities, notably smaller or rural institutions, face staffing shortages, limited analytical tools, training gaps, and competition for scarce resources. These constraints reduce their ability to keep pace with evolving terrorist financing risks and fully engage in PPC. As a result, report processing is delayed, reporting quality becomes inconsistent, and participation in PPCs is uneven across sectors.

Practical Solutions

- i. Adopt tiered, risk-based pathways: Jurisdictions should adopt staged and proportionate pathways such as Lao PDR's four-step model: beginning with national risk and gap assessments, establishing structured dialogue platforms, piloting information-sharing mechanisms, and formalising frameworks once effectiveness is demonstrated.
- ii. Provide scalable, standardised guidance and templates: FIUs and supervisors should provide reporting entities with standardised templates, model agreements, procedural guidance, and risk-based supervisory expectations that can be adapted to the local context.
- iii. Invest in sustained capacity building across sectors: Jurisdictions should institutionalise regular joint training programmes to ensure consistent capability in risk identification, reporting, and analysis.

5. Cultural and Linguistic Differences

Public-private cooperation depends on clarity of language, shared understanding, and trust. However, terminology differs across sectors and between jurisdictions, and translation gaps can lead to misunderstandings. In other cases, hierarchical cultures might discourage open information exchange.

Practical Solutions

- i. Create shared operational language: this includes standard typology definitions, a terminology guide, and clarity on thresholds and expectations.
 - ii. Prioritise relationship-building through repeated engagement, face-to-face workshops, informal channels, and structured feedback.
 - iii. Promote peer-to-peer learning with engagement encouraged from all PPC members on terrorist financing detection and disruption methods, tools, and techniques.
-

6. Financial Inclusion and Unintended Consequences

Financial inclusion impacts are a high priority for the region, and concerns exist about de-risking by jurisdictions and the debanking of specific individuals and entities (such as legitimate humanitarian NGOs/NPOs) and women-led organisations, as well as the ultimate impact of shifting financial transactions into unregulated channels.⁷⁰ Operationally, financial exclusion increases terrorist-financing risks by reducing transaction transparency.

Practical Solutions

- i. Consistent application of a risk-based approach: financial institutions and supervisors should assess customers and activities based on objective and individualised risk assessments, avoiding blanket exclusion of whole sectors or customer groups. This ensures proportionate controls while preserving access to legitimate financial services.
- ii. Build structured engagement with the NGO/NPO sector: authorities and financial institutions should establish ongoing dialogue and cooperation with non-government/non-profit organisations to understand risk, share guidance, and prevent both abuse and unnecessary disruption to legitimate activities. This can include developing localised Recommendation 8 and terrorist financing handbooks or manuals to help them develop their internal controls, as well as continuous engagement and support from charity/NPO regulators that can help prevent exploitation of legitimate NPOs and support detection of terrorist financing through misuse of NPOs.
- iii. Monitor and review unintended consequences: using surveys, reporting metrics, and appeal/review mechanisms to identify and resolve harm as it emerges.
- iv. Embed gender-aware analysis: authorities and reporting entities should recognise that terrorist financing risks and regulatory impacts can differ by gender, including women acting as facilitators or being unintentionally excluded from financial systems due to documentation barriers. Integrating gender awareness supports both human-rights obligations and more accurate risk assessment.

The most effective public-private partnerships recognise that challenges related to technology, law, trust, capacity, and financial inclusion are deeply interconnected. Practical solutions, therefore, require a combination of clear legal authority, secure technology, sustained relationship building, structured feedback processes, regional coordination, and inclusive, proportionate regulation.

Survey findings confirm that practitioners favour balanced hybrid models that integrate formal frameworks with informal collaboration, because this approach reflects operational reality and supports timely response. The overarching lesson is that speed, trust, and clarity save lives. Counter terrorist financing cooperation must therefore be designed not only to meet regulatory requirements, but also to enable rapid, lawful, and intelligence-driven prevention of terrorist financing across borders.

⁷⁰ United Nations Global Counter-Terrorism Coordination Compact. 2025, "[Guidance on Ensuring Respect for Human Rights while Taking Measures to Counter the Financing of Terrorism](#)". Co-led by the Counter-Terrorism Committee Executive Directorate and the Office of the United Nations High Commissioner for Human Rights. United Nations. 2025.

Conclusion

PPC mechanisms that enable the exchange of intelligence in real-time investigations and strengthen mutual understanding of risk and typologies, contribute to robust and effective systems to counter the financing of terrorism. As the financial system evolves and terrorists diversify methods to finance their activities, the value of such mechanisms only increases.

While formal PPC frameworks remain a long-term goal, substantial progress can be achieved through practical, lower-threshold initiatives that do not require legislative reform or formal data-sharing agreements. Investment in building trust, strengthening analytical capability, and creating a shared understanding of terrorist financing risks across both public authorities and private-sector reporting entities can bring significant short-term benefits and lay the foundations for formalised and operational information sharing in the longer-term.

By adopting an incremental approach, systems can be adapted to fit the jurisdictional context ensuring a proportionate response to national and sectoral risk through measures that are realistic, sustainable and aligned with available resources. Training plays a pivotal role in this process, contributing to a shared understanding of terrorist financing risks and trends while providing a forum for developing trust between institutions.

At the regional level, even absent harmonised regulatory frameworks across jurisdictions, common minimum standards and understanding can support information sharing and a move away from siloed practice. Organisations including ASEAN and the Egmont Group can play a crucial role in this process.

Privacy and data protection regulations provide vital safeguards in the context of increasing generation of personal data. These safeguards must be respected while enabling lawful, necessary and proportionate information sharing to combat the threat posed by terrorist financing.

Annex 1: Case Studies: Establishing PPC Frameworks for Counter-Terrorist Financing

Case Study 1: Australia's FINTEL Alliance - Co-Location Model

Framework Overview

Australia's FIU, the Australian Transaction Report and Analysis Centre (AUSTRAC), established the FINTEL Alliance as a PPC in March 2017 to address financial crime, including terrorism financing. The Alliance operates under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006, which provides explicit legal authority for information sharing between government agencies and private sector entities.⁷¹

Governance and Membership

AUSTRAC leads the Alliance through a steering committee responsible for strategic oversight, supported by working groups that address specific threat areas including terrorism financing and child exploitation.⁷² Rather than maintaining permanent structures for every contingency, AUSTRAC forms taskforces as priorities emerge, which keeps the model flexible.

Government participants include AUSTRAC, Australian Federal Police, Australian Border Force, Australian Tax Office and Australian Security Intelligence Organisation. On the private sector side, the core membership comprises Australia's major banks including ANZ, Westpac, NAB, Commonwealth Bank of Australia, HSBC, Citibank, with participation subsequently expanded to include casinos, remittance providers and fintech companies.⁷³ This broader membership reflects the reality that financial crime does not confine itself to traditional banking channels.

How It Works

What distinguishes the FINTEL Alliance from many other partnership models is co-location.⁷⁴ Private sector analysts work at AUSTRAC headquarters alongside government intelligence officers, which means emerging patterns can be discussed immediately. The team can respond in near real-time, sharing both strategic intelligence such as typologies and red-flag indicators, as well as operational intelligence on active cases.⁷⁵

Cases typically begin with suspicious transaction reports, intelligence leads or awareness of emerging threats. AUSTRAC leads investigations with input from federal police and banks. Other government agencies exercise investigative powers, conduct prosecutions and manage intelligence dissemination, while banks monitor transactions, provide customer data and perform real-time analysis. Each contributes what it is best positioned to do.⁷⁶

⁷¹ See: AUSTRAC, "Fintel Alliance," AUSTRAC [website](#).

⁷² *Ibid*

⁷³ AUSTRAC, "Fintel Alliance," AUSTRAC website, [partner list](#); United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), "[Analytical Brief: Establishing Effective Public-Private Partnerships on Countering the Financing of Terrorism](#)". December 2023.

⁷⁴ Maxwell, Nick J. and Artingstall, David, "[The Role of Financial Information-Sharing Partnerships in the Disruption of Crime](#)". Royal United Services Institute, October 2017.

⁷⁵ *Ibid*

⁷⁶ "[Private Sector Information Sharing](#)": FATF, November 2017 and [AUSTRAC Annual Report 2021-22](#). Commonwealth of Australia, 2022.

What Makes It Work

Government funding through AUSTRAC's budget provides stability, while private sector contributions, such as seconded analysts, data access, and compliance expertise add substantial value.⁷⁷ This secondment model works because institutions can justify contributing human resources more readily than making direct financial payments to what might otherwise appear to be government functions.⁷⁸

Legislative clarity has proved equally important. Before the relevant amendments, institutions faced a genuine paradox: cooperating with law enforcement could expose them to regulatory liability even when their cooperation led to successful investigations. Explicit statutory protection for appropriate information sharing resolved this, and the lesson is transferable. Attempting partnerships without a clear legal foundation creates liability exposure that prevents meaningful private sector participation regardless of how much goodwill exists on either side.⁷⁹

Results

Fintel Alliance has delivered concrete outcomes. It disrupted an IS-linked remittance network in 2019 and developed child exploitation financing typologies that have since been circulated internationally.⁸⁰ The quality of suspicious transaction reporting has improved as banks have gained clearer understanding of investigative priorities through sustained collaboration.⁸¹ More fundamentally, the partnership shifted the operating model from reactive reporting to proactive intelligence sharing, which represents a meaningful change in how public and private sectors cooperate against financial crime.

Challenges

Privacy restrictions present the first major challenge, limiting what customer data can be shared and requiring careful protocols that distinguish actionable intelligence from protected personal information.⁸² The co-location model, while highly effective, requires sustained resource commitments that may not be feasible for all institutions, and smaller firms in particular have found it difficult to second staff for extended periods.⁸³ Cultural resistance between banks and government required sustained trust-building in the Alliance's early years, which is worth anticipating in any comparable initiative.⁸⁴

Cross-border cooperation remains the most persistent challenge. The Alliance handles domestic threats and those with clear Australian connections effectively, but intelligence sharing with foreign FIUs or banks faces legal barriers that international criminal networks can exploit.⁸⁵

⁷⁷ *Ibid* and Maxwell and Artingstall at fn. 74

⁷⁸ FATF, "Private Sector Information Sharing" at fn. 76 and CTED, "Analytical Brief" at fn. 73.

⁷⁹ *Ibid*

⁸⁰ Fn. 15

⁸¹ Australian Transaction Reports and Analysis Centre, Annual Report 2021-22 at fn. 76

⁸² FATF, "Private Sector Information Sharing" at fn. 78 and CTED, "Analytical Brief" at fn. 73.

⁸³ Maxwell and Artingstall, at fn. 76 and "[Preventing Money Laundering and Terrorist Financing: A Practical Guide for Bank Supervisors](#)", World Bank Group, 2022.

⁸⁴ Fn. 74

⁸⁵ CTED Analytical Brief at fn. 73; See also "[Public-Private Partnerships Role of FIUs in PPPs](#)". Egmont Group of Financial Intelligence Units.

Lessons for Southeast Asia

Jurisdictions considering similar models might consider initially concentrating on strategic intelligence sharing, focusing on typologies and red flags indicators, rather than attempting full operational cooperation from the outset. Lower-sensitivity information builds trust while legal frameworks develop, and participants learn to collaborate effectively. This graduated approach allows partnerships to demonstrate value before tackling more complex operational challenges.⁸⁶

Co-location, while valuable, is one approach among several. What proves essential is regular and sustained engagement rather than physical location. Jurisdictions should adopt mechanisms suited to their resources and national contexts, with the priority being ongoing interaction that maintains relationships and demonstrates continued value to participants, especially considering Southeast Asia's complex cross-border relationships.⁸⁷

Strong FIU capacity is a prerequisite, not an optional feature.⁸⁸ AUSTRAC commands respect from both government agencies and private institutions because it combines regulatory authority with strong analytical capability. Jurisdictions with developing FIUs should invest in institutional strengthening before attempting complex partnerships, as the coordinating body sets the ceiling for what the partnership can achieve.⁸⁹

Most critically, legislative reform should precede operational cooperation. Without a clear legal foundation, liability exposure prevents meaningful private sector engagement, regardless of operational necessity or regulatory encouragement.

⁸⁶ CTED Analytical Brief at fn. 73

⁸⁷ *Ibid* and Maxwell and Artingstall at fn. 74.

⁸⁸ FATF, "Private Sector Information Sharing" at fn. 76.

⁸⁹ *Ibid*

Case Study 2: Hong Kong's FMLIT - Phased Expansion Approach

Framework Overview

The Fraud and Money Laundering Intelligence Taskforce (FMLIT) was launched on 26 May 2017 as a 12-month pilot, led by the Hong Kong Police Force Commercial Crime Bureau in collaboration with the Hong Kong Monetary Authority (HKMA) and the banking industry.⁹⁰ The pilot approach allowed authorities to test the model before committing to permanent implementation. Following its success, the initiative expanded to include virtual banks.⁹¹

Legal Foundation

FFMLIT operates under Section 25A of the Organised and Serious Crimes Ordinance, which governs reporting of criminal property. This provision excludes liability for breach of contract or other liability for damages arising from any loss incurred because of the disclosure.⁹² Section 25A links to Section 25, which criminalises dealing with criminal property but provides a defence where disclosure is intended under Section 25A.⁹³

Governance and Membership

FMLIT's governance structure is divided into two groups with distinct functions:

- i. The Strategic Group brings together senior representatives from law enforcement, the HKMA and the banking industry.
- ii. The Operations Group focuses on cases, with intelligence professionals from banks and law enforcement working side by side.

How It Works

The Strategic Group meets every six months to agree on priority threats and assess whether the initiative justifies continued investment, while the Operations Group meets monthly to maintain regular engagement. Banks detect unusual customer flows or mule account behaviour through their monitoring systems and submit intelligence to the Operations Group. Law enforcement engages when investigations develop beyond preliminary assessments, with intelligence staff from participating banks working directly with law enforcement to identify patterns spanning multiple institutions, that neither sector could have detected working alone.

The Operations Group decides whether cases warrant escalation to full law enforcement operations based on evidence strength and resource availability. FMLIT does not itself conduct law enforcement operations, but the monthly tactical meetings enable near real-time intelligence sharing, allowing banks to act quickly, including suspending suspicious accounts before formal police action begins.

Information sharing operates at different sensitivity levels. The Alert Function circulates anonymised typology reports to the wider banking industry through Hong Kong Association of Banks' channels, enabling banks to detect trends in fraud, trade-based money laundering and mule account networks without requiring full taskforce membership. Anonymised case data of medium sensitivity circulates among Operations Group participants. While anything involving potentially identifiable details requires joint approval from law enforcement and banks before being shared.

⁹⁰ HKMA, "Fraud and Money Laundering Intelligence Taskforce launched," Hong Kong Monetary Authority, Press Release, 26 May 2017.

⁹¹ Or, Sara S. M., "Fighting digital fraud with enhanced approaches in Hong Kong" JSM, 2023.

⁹² Cap. 455 Organized and Serious Crimes Ordinance

⁹³ *Ibid*

Results

FMLIT collaboration has enabled banks and law enforcement to map large mule account networks and criminal flows that individual institutions working independently could not have detected. By June 2023, FMLIT had identified over 21,000 previously unknown mule accounts used to move illicit funds.⁹⁴ Between 2017 and 2023, the initiative led to approximately HK\$1.1 billion in crime proceeds being restrained or confiscated, with HK\$700 million restricted by September 2021 alone.⁹⁵

FMLIT is publicly framed around fraud and money laundering rather than terrorism financing specifically but disrupting mule account networks and fraud-related money laundering flows contributes indirectly to CTF by cutting off funding channels that terrorist actors could potentially exploit.

Challenges

FMLIT operates without dedicated public funding. Partners are required to allocate resources from existing budgets through staff secondments, data sharing and operational cooperation, which constrains scalability.⁹⁶ The number of fully operational cases remains modest relative to overall threat volume, reflecting resource limitations.⁹⁷

Initial reluctance to share sensitive customer information due to confidentiality concerns and competitive considerations meant trust-building was a significant early challenge.⁹⁸ Banks must navigate the Personal Data (Privacy) Ordinance and banking secrecy obligations, which means alerts continue to be limited to anonymised or aggregated data in some circumstances.

Cross-border coordination remains difficult despite strong domestic cooperation. FMLIT functions well within Hong Kong's banking sector but sharing across jurisdictions requires legal agreements that are still being developed.

Lessons for Southeast Asia

FMLIT demonstrates that a PPC structure involving regulators, law enforcement, and banks can function effectively in a major financial centre. The phased approach, beginning with a 12-month pilot involving ten major retail banks, was key to establishing the model's credibility before broader implementation.

The two-tier governance system is effective. Senior representatives set strategic direction through the Strategic Group, while intelligence professionals develop operational cases through the Operations Group. Keeping these functions separate allows each level to focus on what it does best. The Alert Function similarly illustrates how information sharing can operate at multiple levels simultaneously, with strategic intelligence circulating industry-wide through anonymised typology reports while operational intelligence on specific cases remains restricted to core participants. Broader threat awareness does not require every institution to participate in operational casework.

Critical success factors include a strong central regulator or FIU to coordinate efforts, legal frameworks that enable information sharing while protecting privacy, secure communications infrastructure, regular coordination meetings, active bank engagement, and in-kind resource commitments from participants.⁹⁹

⁹⁴ Yue, Eddie, "How banks can contribute more to the fight against fraud and money laundering," Hong Kong Monetary Authority, 2024.

⁹⁵ "The HKMA hosts Anti-Money Laundering Webinar on Collaboration, Data and Technology", Hong Kong Monetary Authority press release, 2021,. See also, "LCQ21: Fraud and Money Laundering Intelligence Taskforce," Hong Kong Government Information Services Department press release, April 21, 2023. And Maxwell, Nick J, "Expanding the Capability of Financial Information-Sharing Partnerships," Royal United Services Institute, 2019,

⁹⁶ Maxwell, Nick, and Artingstall, David. "Expanding the Capability of Financial Information-Sharing Partnerships" Royal United Services Institute, 2019.

⁹⁷ Yue at fn. 94 and *Ibid*.

⁹⁸ FMLIT's information sharing arrangements operated within the constraints of Hong Kong's Personal Data (Privacy) Ordinance and banking secrecy obligations, with anonymisation serving as a practical workaround rather than a positively authorised framework. As of January 2024, the HKMA was consulting on legislative amendments to create a clearer legal basis for bank-to-bank information sharing. See also Yue at fn. 94.

⁹⁹ Maxwell and Artingstall at fn. 96 and "Hong Kong Monetary Authority and Hong Kong Police Force Co-host Sharing Session with Banking Industry on Anti-Deception Efforts," Press Release, April 21, 2023.

Case Study 3: Malaysia's MyFINet - Central Bank Leadership Model

Framework Overview

Malaysia established the Malaysia Financial Intelligence Network (MyFINet) in 2017 and formally launched it on 5 November 2019. This initiative, led by the Financial Intelligence Unit of Bank Negara Malaysia (BNM, the Central Bank of Malaysia), brings together law enforcement agencies and financial institutions to counter money laundering, terrorism financing, proliferation financing and other serious crimes. MyFINet comprises multiple thematic working groups that focus on specific crime types, including terrorism financing.

Legal Foundation

MyFINet operates within the legal framework of the Anti-Money Laundering, Anti-Terrorism Financing, Anti-Restricted Activity Financing and Proceeds of Unlawful Activities Act 2001. The existing legislative framework provides sufficient legal basis for reporting obligations and confidentiality requirements, without the need for new legislation.

Governance and Membership

MyFINet was established as part of the National Strategic AML/CFT Plan 2015-2020 under the purview of the National Coordination Committee to Counter Money Laundering (NCC). Each MyFINet working group operates in accordance with its own Terms of Reference.

Public sector members include BNM, the Royal Malaysia Police, the Malaysian Anti-Corruption Commission, the Securities Commission Malaysia, the Royal Malaysian Customs Department and the Inland Revenue Board of Malaysia. Private sector members comprise selected banks, electronic wallet providers, remittance service providers, designated non-financial businesses and professions, and digital asset exchangers. The inclusion of non-bank financial service providers from the outset reflects the recognition that financial crime is not confined to traditional banking channels. It also helps ensure that the framework remains relevant as financial activities and transactions increasingly migrate to emerging platforms.

How It Works

MyFINet operates through working groups that primarily focus on tactical intelligence relating to specific cases as initiated by law enforcement agencies. Under this initiative, the FIU facilitates discussions and meetings between law enforcement agencies and financial institutions. During these meetings, the respective law enforcement agencies share specific intelligence, red-flags, and typologies with selected financial institutions. Based on the information shared, the financial institutions support the law enforcement investigations through the enhanced identification and reporting of suspicious transactions to the FIU. The Financial Intelligence System is a secure platform for the exchange of sensitive information relating to cases discussed during these meetings.

Results

MyFINet has enhanced law enforcement outcomes by supporting investigations, prosecutions, asset recovery efforts and other measures aimed at disrupting criminal networks. The collaboration has resulted in reporting institutions submitting higher-quality and more targeted TF-related Suspicious Transaction Reports (STRs). At the same time, reporting institutions benefit from strategic intelligence shared by public sector agencies, including information on modus operandi, red flags, and typologies which strengthens their ability to identify and detect TF-related transactions. As a result, subjects of interest that were previously not identified through customer due diligence or transaction monitoring processes, due to low transaction values or otherwise unremarkable customer profiles, are now being detected, monitored and reported.

Since 2017, the MyFINet TF Working Group has achieved several notable outcomes, including: (i) the arrest and prosecution of 21 individuals for TF activities, (ii) the arrest and deportation of two foreign nationals; and (iii) a significant increase in the number of TF-related STRs.¹⁰⁰

Challenges

The sheer volume of data requires continued investment in analytics, real-time monitoring and cross-entity analysis. The FIU has adopted data analytics to prioritise STRs based on risk profiles and has developed a network analysis tool to identify linkages between criminal actors across multiple databases. However, there remains a need to further enhance its STR triage algorithm by incorporating inputs from stakeholders and users, including reporting institutions, law enforcement agencies and other subject matter experts. This will help ensure that relevant intelligence is identified, prioritised and surfaced effectively and efficiently.

Lessons for Southeast Asia

MyFINet illustrates the impact that can be achieved when a central regulator and FIU possess both the authority and institutional credibility to bring together stakeholders from across the public and private sectors. BNM's dual role is not incidental to the success of the model; it is a fundamental enabler. Jurisdictions without a similarly positioned FIU may face challenges in sustaining a comparable level of coordination and collaboration.

The NCC governance structure is crucial. Managing the competing priorities of law enforcement agencies, financial regulators, and private sector participants requires more than a consultative platform; it necessitates a forum with sufficient authority to provide strategic direction and facilitate decision making.

The inclusion of non-bank financial institutions in MYFINet from the outset has proven to be more effective than retrofitting them into an existing bank-focused framework.

On the technology front, the data analytical and network analysis tools employed by BNM are essential for processing large volumes of data.¹⁰¹ In practice, however, building and sustaining these capabilities requires continuous investment and specialised expertise. Jurisdictions seeking to replicate the model may prefer a phased approach, rather than treating advanced analytics as a prerequisite.¹⁰²

MyFINet's success is underpinned by several key factors, including strong trust between the public and private sectors; secure analytical and information-sharing infrastructure; active private sector participation spanning banks, FinTech's and payment service providers; a legal framework that enables information sharing while safeguarding confidentiality and data protection; and analytical capabilities for processing large volumes of financial crime data.

¹⁰⁰ **Malaysia: Mutual Evaluation Report**, Asia Pacific Group on Money Laundering, 2025.

¹⁰¹ Yusoff, Yusri Hazrol, Fatin Syasya Md Zamri, Nur Alia Izzati Mohd Yusri, Nur Syafinaz Shaharudin, and Syafiqah Sorfina Abdullah. "The Elements Affecting the Anti-Money Laundering Practices Efficiency in Malaysia's Business Sector." *International Journal of Research and Innovation in Social Science* 8, no. 10, 2024.

¹⁰² Anuar, A. N. B., Saari, S. S. B., Khaidir, G. R. B., & Yusoff, Y. H. "Examining compliance cost challenges in suspicious transaction reporting among financial institutions in Malaysia: A concept paper". *International Journal of Research and Innovation in Social Science*, 2025.

Annex 2: Enabling Documents (Draft Templates)

Draft MoU for Strategic Information Sharing

Memorandum of Understanding: Strategic Cooperation on Counter-Terrorist Financing

This Memorandum of Understanding (“MoU”) is entered into between **[Name of Financial Intelligence Unit]** (the “FIU”) and **[Name of Financial Institution]** (the “FI”), together referred to as the “Parties.”

The purpose of this MoU is to establish a framework for voluntary cooperation and the exchange of strategic, non-operational information related to counter-terrorist financing (CTF). Through this cooperation, the Parties seek to improve their shared understanding of terrorist-financing threats, risks, and typologies, and to strengthen the effectiveness of risk-based AML/CTF controls through public-private cooperation (PPC). This MoU does not provide for the sharing of operational, investigative, or case-specific information.

This MOU is concluded in accordance with the FIU’s statutory mandate to receive, analyse, and disseminate financial intelligence and to engage in strategic outreach, and the Bank’s authority to manage AML/CTF risks in accordance with applicable laws and regulations.¹⁰³ Nothing in this MOU is intended to override or amend existing legal or regulatory obligations, create new reporting or supervisory requirements, or alter [name of institution] obligation to submit reports as required by law.

The cooperation envisaged under this MOU is limited to the exchange of strategic, non-operational, and non-identifying information. The FIU may share strategic assessments of terrorist-financing threats and trends, typologies and red-flag indicators, aggregated or anonymised reporting trends, sector-specific or geographic risk insights, and strategic briefings following significant developments relevant to terrorist financing. The Bank may share aggregated and anonymised observations related to terrorist-financing risks, including product, service, or delivery-channel vulnerabilities, challenges encountered in detecting terrorist-financing activity, and feedback on the clarity and usefulness of typologies and strategic guidance.

The Parties agree that no personal identifiable information shall be exchanged under this MOU. This includes, but is not limited to, customer-specific, account-level, or transaction-level data; the names of customers, entities, or beneficial owners; information relating to ongoing investigations or enforcement actions; or any information intended for operational or evidentiary use.

Information exchanged pursuant to this MOU may be used solely for internal AML/CTF risk assessment, strategic analysis, and the enhancement of policies, controls, and compliance frameworks. Such information shall not be construed as supervisory instruction, legal advice, or direction to file or refrain from filing any report and shall not be relied upon as the sole basis for customer-level or compliance decisions without independent analysis. Each Party shall treat information received under this MOU as confidential and shall apply appropriate administrative, technical, and organisational safeguards to protect it from unauthorised access or disclosure.¹⁰⁴ Information shall not be shared onward with third parties without the prior written consent of the originating Party, unless disclosure is required by law.

¹⁰³ Refer to relevant legislation here

¹⁰⁴ Insert reference to any information / security legislation here.

Strategic information may be exchanged through written analytical products, strategic briefings, workshops, roundtables, or other agreed non-operational channels. The Parties may also engage in periodic discussions to support mutual understanding of terrorist-financing risks and emerging trends. Each Party shall designate a point of contact responsible for coordinating cooperation under this MOU.

This MOU shall enter into force on the date of signature and shall remain in effect for a period of [X] years, unless terminated earlier by either Party upon [X] days' written notice. The confidentiality obligations set out in this MOU shall survive its termination. The Parties may review this MOU periodically to ensure that it remains relevant and aligned with evolving terrorist-financing risks and international standards, including those of the Financial Action Task Force.

Signed on behalf of the Parties by their duly authorised representatives.

For the Financial Intelligence Unit

Name:

Title:

Date:

For the Financial Institution

Name:

Title:

Date:

Draft MoU for Operational Information Sharing

Memorandum of Understanding: Operational Cooperation on Counter-Terrorist Financing

This Memorandum of Understanding ("MoU") is entered into between **[Name of Financial Intelligence Unit]** (the "FIU") and **[Name of Financial Institution]** (the "FI"), together referred to as the "Parties."

The purpose of this MoU is to establish a framework for operational cooperation and limited information exchange related to counter-terrorist financing (CTF) to support the timely detection, analysis, and disruption of terrorist-financing activity. This cooperation is intended to enhance public-private cooperation (PPCs) while preserving the distinct roles, responsibilities, and legal authorities of each Party.

This MOU is concluded in accordance with the FIU's statutory mandate to receive, analyse, and disseminate financial intelligence and to cooperate with reporting entities for the purposes of combating terrorist financing, and the Bank's authority and obligations to identify, assess, and report suspicious activity under applicable law.¹⁰⁵ Nothing in this MOU is intended to override or amend existing legal or regulatory obligations, create new reporting requirements, or alter the Bank's independent obligation to submit suspicious transaction reports in accordance with applicable law.

The cooperation envisaged under this MOU permits the exchange of operationally relevant information, subject to strict legal and procedural safeguards. The FIU may share operational alerts, priority threat indicators, risk narratives linked to active terrorist-financing threats, feedback related to submitted reports, and contextual information intended to assist the Bank in identifying activity of potential relevance to terrorist financing. The FIU may also issue time-bound alerts following terrorist incidents, designations, or emerging threats, requesting heightened vigilance in relation to specified typologies, methods, or risk vectors.

¹⁰⁵ References to relevant laws here.

The Bank may share information in response to such alerts or requests, including relevant transactional, customer, or account information, where permitted by law and as necessary for the FIU's analysis of terrorist-financing activity. The Bank may also provide clarifications or supplementary information related to previously submitted reports, as well as operational feedback on the feasibility and impact of alerts or requests. Nothing in this MOU shall be interpreted as requiring the Bank to conduct investigations on behalf of the FIU or law enforcement.

Information exchanged under this MOU shall be limited to what is necessary and proportionate for CTF purposes. The Parties acknowledge that operational information may include sensitive or identifying data and agree that such information shall be handled in accordance with applicable confidentiality, data-protection, and banking-secrecy laws.¹⁰⁶ Access to operational information shall be restricted to authorised personnel with a demonstrated need to know, and appropriate technical and organisational safeguards shall be applied to prevent unauthorised access, use, or disclosure.

Information shared pursuant to this MOU may be used by the FIU solely for intelligence analysis, dissemination in accordance with its legal mandate, and the support of CTF efforts. Information shared by the FIU may be used by the Bank solely for AML/CTF compliance, risk management, and reporting purposes. Information exchanged under this MOU shall not be used for commercial purposes or as the sole basis for adverse customer action without independent analysis and, where applicable, additional corroborating information.

The Parties acknowledge that the submission of information under this MOU does not replace, delay, or pre-empt the Bank's obligation to file suspicious transaction reports, nor does it constitute confirmation that any activity is or is not linked to terrorist financing. Decisions regarding reporting remain the sole responsibility of the Bank.

Operational information may be exchanged through secure communication channels agreed by the Parties, including secure electronic systems, designated points of contact, or other controlled mechanisms. Each Party shall designate primary and alternate operational points of contact responsible for coordinating requests, responses, and follow-up under this MOU.

This MOU shall enter into force on the date of signature and shall remain in effect for a period of [X] years, unless terminated earlier by either Party upon [X] days' written notice. The obligations relating to confidentiality, data protection, and permitted use of information shall survive termination. The Parties may review this MOU periodically to ensure continued relevance, effectiveness, and alignment with evolving terrorist-financing risks and international standards, including those of the Financial Action Task Force.

Signed on behalf of the Parties by their duly authorised representatives.

For the Financial Intelligence Unit

Name:

Title:

Date:

For the Financial Institution

Name:

Title:

Date:

¹⁰⁶ Relevant national legislation referenced here.

Tool: PPC Membership Design Checklist (Threat-Led Approach)

Purpose:

This tool supports competent authorities in designing PPC membership based on the specific terrorist financing threat environment. It ensures participation is targeted, proportionate, and capability-driven, aligning the right actors to the right threat and intended function (operational or strategic).

1. Define the PPC Model

- Is the PPC primarily **operational**, **strategic**, or both?
- Are the objectives clearly defined and aligned with the chosen model?

2. Define the Threat

- Clearly describe the terrorist financing threat (actors, networks, geographies)
- Identify key financing methods (e.g., banking, cash, crypto, NPOs, online platforms)
- Map the relevant financial lifecycle stages (raising, using, moving, storing, managing, hiding)
- Assess whether the threat is domestic, cross-border, or hybrid

3. Confirm Core Participants

- Financial intelligence unit(s) (FIUs)
- Law enforcement / investigative authorities
- Relevant financial institutions and reporting entities
- Coverage of key financial channels relevant to the threat

4. Assess Additional / Context-Specific Participants

- Technology and communications actors (e.g., social media, ISPs, platforms)
- Sector-specific actors (e.g., payment processors, travel sector, crypto providers)
- NPO regulators or umbrella bodies (as appropriate)
- Other relevant domestic or international partners
- Use of consortium or representative bodies where direct participation is not appropriate

5. Define Roles and Value Added

- Clearly articulate each participant's role
 - Identify the data, expertise, or capability contributed
-

Further Readings and Resources

1. **The APMG Public-Private Partnership (PPP) Certification Guide:** General guide on creating a PPP framework. <https://ppp-certification.com/pppguide-v2/download>
 2. **EFIPPP Practical Guide for Operational Cooperation between Investigative Authorities and Financial Institutions;** January 2025. <https://www.europol.europa.eu/publications-events/publications/efippp-practical-guide-for-operational-cooperation-between-investigative-authorities-and-financial-institutions>
 3. **Public-Private Partnership Toolkit Against Organized Fraud.** UNODC, 2026. https://www.unodc.org/res/organized-crime/GFS/publications/UNODC_Public-Private_Partnership_Toolkit_Against_Organized_Fraud_EN.pdf
 4. **Compendium – Public Private Partnerships in the Drug Control Area.** UNODC Drug Research Section. 30 December 2021. https://www.unodc.org/documents/donors/Public_private_partnership.pdf
 5. **Establishing Effective Public-Private Partnerships on Countering the Financing of Terrorism.** United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), 2023. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/cted_analytical_brief_on_ppps_cft_2023.pdf
 6. **Evaluating the Effectiveness of Public-Private Partnerships in Anti-Money Laundering: U.S. Case Studies, Global Insights, and Policy Implications.** Samuel Aidoo, 2025. https://www.researchgate.net/publication/393655274_Evaluating_the_Effectiveness_of_Public-Private_Partnerships_in_Anti-Money_Laundering_US_Case_Studies_Global_Insights_and_Policy_Implications
 7. **The Path Forward for effective public-private partnerships in drug control.** UNODC, 2022. <https://www.unodc.org/documents/donors/PPPfactsheet-Proceeds-Narcotrafficking-WEB.pdf>
 8. **Preventing Money Laundering and Terrorist Financing. A practical guide for bank supervisors.** Second Edition. World Bank Group, 2022. <https://documents1.worldbank.org/curated/en/099532507212213583/pdf/IDU04f85b34a0f6dc04f19083f307136897d2cb6.pdf>
 9. **Private Sector Information Sharing.** FATF, 2017. <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private-Sector-Information-Sharing.pdf.coredownload.pdf>
 10. **Public-Private Partnerships. Role of FIUs in PPPs.** Egmont Group, 2021. https://egmontgroup.org/wp-content/uploads/2021/09/2018_Public-Private_Partnerships_PPPs_from_the_perspective_of_Financial_Intelligence_Units_FIUs.pdf
 11. **Public-Private Security Cooperation. From Cyber to Financial Crime.** Hugo Rosemont. Royal United Services Institute, 2016. <https://static.rusi.org/OP-201608-Rosemont-PublicPrivate-Security-Cooperation1.pdf>
 12. **The Role of Financial Information-Sharing Partnerships in the Disruption of Crime.** Nick J Maxwell and David Artingstall. Royal United Services Institute, 2017.
 13. **Terrorist Financing Risk Assessment Guidance.** FATF, 2019. <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Terrorist-Financing-Risk-Assessment-Guidance.pdf>
 14. **Chapter 2: The Role of the Private Sector in Detecting and Disrupting Terrorist Financing Activities; Countering the Financing of Terrorism Good Practices to Enhance Effectiveness:** Arz El Murr, Terence Donovan and Yee Man Yu. International Monetary Fund, 2023. <https://www.elibrary.imf.org/display/book/9798400204654/CH002.xml>
 15. **Public-Private Partnerships for Financial Information Sharing; U4 Helpdesk Answer 2025:** Dolan, Carl and Bergin, Jamie. https://knowledgehub.transparencycdn.org/kproducts/PPP-for-financial-info-sharing_ForPublishing.pdf
 16. **Developing Public-Private Information Sharing to Strengthen the Fight against Money Laundering and Terrorism Financing, Recommendations for the European Union.** Benjamin Vogel, Maxime Lassalle. Max Planck Institute for the Study of Crime, Security and Law, 2024. <https://doi.org/10.30709/eucrim-2023-031>
-



The International Institute for Justice and the Rule of Law

University of Malta - Valletta Campus
Old University Building, St. Paul Street, Valletta, Malta

info@theiij.org  @iijmalta **www.theiij.org**