FATF

FATF Report

Information Sharing to Combat Illicit Finance

Global Overview of Public and Private Sector Partnerships and Data Protection Arrangements

July 2026

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2026), *Information Sharing to Combat Illicit Finance: Global Overview of Public and Private Sector Partnerships and Data Protection Arrangements,* FATF, France, www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/information-sharing-ppp-data-protection-arrangements

Table of contents

Abbreviations and Acronyms

AI	Artificial Intelligence
AML	Anti-Money Laundering
API	Application Programming Interface
CDD	Customer Due Diligence
CFT	Countering the financing of terrorism
CTAF	Tunisian Financial Analysis Committee
DPA	Data protection authority
DPIA	Data protection impact assessment
DPP	Data protection and privacy
DNFBP	Designated non-financial businesses and professions
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
FATF	Financial Action Task Force
FSRB	FATF-Style Regional Body
FI	Financial institution
FinCEN	Financial Crimes Enforcement Network (US)
FIU	Financial intelligence unit
GDPR	General Data Protection Regulation (EU)
KYC	Know your customer
ISAs	Information sharing agreements
LEA	Law enforcement authority
MER	Mutual evaluation report
ML	Money Laundering
MOU	Memorandum of Understanding
NPO	Non-profit organisation
NRA	National risk assessment
PET	Privacy Enhancing Technology
PPP	Public-private partnership
SAR	Suspicious Activity Report
SPAK	Special Structure against Corruption and Organised Crime
STR	Suspicious Transaction Report
TF	Terrorist financing
UN	United Nations
UN CTED	UN Counter-Terrorism Committee Executive Directorate

Executive Summary

1. In this era of increased digitalisation, and given the speed and complexity of cross-border transactions, effective information sharing between the public and private sector is key for the effectiveness of AML/CFT systems. The paper highlights the urgent need for authorities and the private sector to work together in combatting illicit finance. For example, greater collaboration and speedier information sharing is necessary to address the fraud epidemic and the speed, complexity and scale of the problem. This work illustrates how both public and private sectors are agile and committed to developing joint and enhanced measures to combat crime using PPPs and real time collaboration mechanisms. Over the past decade, PPPs are increasing in prevalence in many jurisdictions, which see the ability of PPPs to significantly enhance trust between the public and private sector and their understanding and mitigation of ML/TF/PF risks. The study further demonstrates how operational PPPs can add particular value, through the rapid exchange of actionable intelligence, and improve the detection and investigation of ML/TF/PF and predicate offences.

2. PPPs are not one-size-fits-all. They take different forms across jurisdictions, varying in purpose, governance, information shared, and outcomes to answer jurisdictions' own needs, capacity and particular circumstances.

3. The report also touches on private-to-private sector information sharing mechanisms and international information sharing arrangements, which remain an area of development for most jurisdictions but are also critical to take more preventative action and holistic responses to illicit finance.

4. Beyond cataloguing jurisdictional approaches (including those highlighted by prior FATF and other publications), the report draws practical insights into what makes PPPs sustainable and especially scalable across different regulatory and cultural contexts to encourage broad implementation across the FATF and its Global Network.

5. Through a comparative analysis of diverse information sharing and PPP models, along with their associated data protection considerations and lessons learned, the report identifies tools and technologies that allow stakeholders to strike a balance between operational efficiency and compliance with data protection, privacy, and human rights obligations. These practices offer valuable guidance for jurisdictions seeking to develop or strengthen frameworks that facilitate collaboration while maintaining data privacy.

6. PPPs are increasingly valued as an effective mechanism to mitigate the risks of criminal activities earlier, moving from a reactive and compliance-based model to a proactive and collaborative one, as they bring together information, resources, technology and specialised expertise that might not be available within a single public agency or private entity. The FATF intends to leverage this report and work on how it can further support development of PPPs so that these tools are fully utilised.

Objective, purpose and structure

7. This document provides a FATF Global Network picture of public-private information sharing practice, presenting different models or mechanisms around the world, recognising no single model of information sharing or PPP fits all jurisdictions.

8. The report highlights key innovations being developed by both newly established and more mature, longstanding PPPs, that demonstrate the evolutionary possibilities regardless of the nature, scale or purpose of each model.

9. This report examines key challenges and considerations faced by developing and established PPPs, along with possible solutions and good practices, key achievements and evidence of added value realisable from collaborative public-private information exchange, across a range of quantitative and qualitative outcomes.

10. This report is intended to assist with information sharing efforts and encourage jurisdictions to engage with one another, to share and learn from each other, to facilitate cooperation, help jurisdictions adopt, replicate or enhance their own models, and improve information sharing while clearly aligning with data protection needs which are key for effective information sharing.

11. The report also considers the types of information shared within PPPs, and the extent to which information can be shared beyond the PPP, including internationally.

12. Importantly, the report does not aim to prescribe a single model of PPP, but to identify common principles and adaptable features that jurisdictions can tailor to their specific needs, as the objective is to provide practical guidance for policymakers and practitioners seeking to establish or refine PPP frameworks that balance operational efficiency, accountability, and respect for fundamental rights.

13. For the purpose of this paper and to help inform future FATF efforts, PPPs are defined as follows:

Box 1. Definition of PPPs

A standing mechanism that enables effective information sharing, collaboration, cooperation, and/or coordination between government authorities with a role in AML/CFT/CPF and the private sector and which may enable information sharing among private sector entities within the framework.

Methodology and participants

14. A diverse project team of 14 FATF Members, eight members of FATF-style Regional Bodies (FSRBs) and five FATF Observers led this work.

15. The report findings are based on:

- A review of open source materials including FATF and other publications cited throughout including mutual evaluation reports.
- Responses to a survey conducted in September 2025, from 78[1] FATF and FSRB delegations including 55 jurisdictions, one organisation, and a multitude of authorities, including financial intelligence units (FIUs), reflecting the variety of agencies responsible for sharing information. Although responses were not received from all FATF and FSRB members of the Global Network (of which there are more than 200), the sample is significant and considered sufficiently representative, covering different continents, legal systems and varying in size and profile of jurisdictions.
- Input requests to participating members and private sector stakeholders, including through desk-based research on policy approaches, industry practices, and case examples and comments received from the FATF and Global Network members during the draft and review process.

16. Responses to survey and other feedback were analysed and embedded in the report without providing references to the owner of the information, in compliance with FATF data protection and privacy rules.

[1] Albania; Angola; Australia; Azerbaijan; Bahrain; Belgium; Benin; Botswana; Brazil; Cyprus; People's Republic of China; Chinese Taipei; Denmark; Eswatini; European Commission; Finland;, Georgia; Ghana; Gibraltar; Greece; Hong Kong, China; India; Indonesia; Iraq; Isle of Man; Italy; Japan; Lao PDR; Latvia; Lesotho; Liberia; Luxembourg; Malta; Moldova;, Marshall Islands; Mexico; Myanmar; Nigeria; North Macedonia; Palestine; Peru; Portugal; Saudi Arabia; South Africa; Seychelles; Singapore; Spain; Sweden; Switzerland; Syria; The Gambia; The Netherlands; Tunisia; United Arab Emirates; the United Kingdom and Zimbabwe.

Background

Pre-existing Global Network knowledge on information sharing mechanisms (public-private, private-private)

17. This report is based on previous work by the FATF and other stakeholders, including:

- FATF's work on the importance of information sharing and revisions to Recommendation 18 and Recommendation 21 in February 2018, as well as guidance for the private sector[2] on information sharing and PPPs.
- FATF's 2022 report on information sharing[3], presenting further case studies on how to increase effective financial crime prevention.

18. The UN CTED released an analytical brief[4] in 2023 outlining PPP frameworks for counter-terrorism financing, highlighting the value of collaborating with multiple stakeholders including social media, to combat crime, as further emphasised in the FATF's 2025 Comprehensive Terrorist Financing Update (CuoTF)[5]. Both the UN Security Council and its Counter-Terrorism Committee strongly encourage national authorities to establish partnerships, in particular with regard to the effective implementation of reporting and disclosure requirements, the use and sharing of relevant financial information from the private sector, and the sharing of information on the evolution of trends, sources and methods of the financing of terrorism.[6] In the context of its 2022 thematic summary assessment of gaps and areas requiring more action to implement key CFT provisions of the relevant Council resolutions,[7] UN CTED noted that most of the States evaluated during the reporting period lacked robust PPPs to share information, understand evolving trends, including to better understand the nexus between terrorism and organised crime, increase knowledge and skills of relevant experts, and strengthen the integrity of the financial sector.

[2] FATF (2017), Guidance on private sector information sharing, FATF, Paris available at: https://www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-information-sharing.html (consulted 17 September 2025).
[3] FATF (2022), Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing, FATF, Paris, France, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf (consulted 22 October 2025).
[4] UN CTED (2023), Establishing Effective Public-Private Partnerships on Countering the Financing of Terrorism, available at: https://www.un-ilibrary.org/content/books/9789211067910. See also materials of the launch expert discussions available at https://www.un.org/securitycouncil/ctc/news/cted-holds-multi-stakeholder-discussion-establishing-effective-public-private-partnerships
[5] FATF (2025), Comprehensive Update on Terrorist Financing Risks, available at: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/comprehensive-update.
[6] Security Council resolution 2462 (2019), para. 22; Delhi Declaration on Countering the Use of New and Emerging Technologies for Terrorist Purposes (Oct. 2022), paras. 15, 25; Algeria Guiding Principles (Jan. 2025), S/2025/22, principles 1(e), 2(g) and (j), 3(l) and (m), 4(e), (g) and (i).
[7] CTED (2022), Thematic summary assessment of gaps in implementing key countering the financing of terrorism provisions of Security Council resolutions, available at: www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/cted_2022_cft_gaps_assessment_final.pdf.

Information sharing mechanisms

Information sharing mechanisms

19. Jurisdictions use different mechanisms to share information between competent authorities and the private sector, and a vast majority include PPPs as part of their information sharing toolkit. Some have more than one PPP for different purposes, and the types of information shared can also vary (e.g. operational or strategic). Only a small portion of jurisdictions surveyed (6[8] out of 50 responding to the survey, which represents a significant sample of Global Network Members) identify as not having PPPs and did not note to have a plan to have one in the near future. Publicly available information also shows strong use of PPPs in additional countries that did not respond to the survey.

20. Jurisdictions with no PPP mechanisms report that secure exchange of information occurs on a regular basis through several alternative mechanisms with their FIUs, between law enforcement and in some cases with the private sector, via encrypted communications, including secure software platforms, as well as Europol and Egmont Secure Web for international information exchange and cooperation (see also Table 1 below). Respondents with PPPs highlighted that some of these same platforms act as important enablers of secure PPP communications.

Table 1. Predominant information sharing mechanisms which can also support PPPs

Model	Characteristics	Stakeholders
FIU-led secure platforms	Usually, operationalised and maintained by the FIU Used by the FIU to collect and share information, including STR/SAR information, financial transactional and due diligence data and FIU analytics outputs/strategic reports Multi-dimensional information flows (i.e. public-public, public-private and private-public) Platforms are generally encrypted, auditable and with access restricted to the relevant stakeholders	FIUs LEAs/Supervisors Reporting entities, including FIs/DNFBPs/VASPs
Judicial/law-enforcement channels	Usually operationalised and maintained by law-enforcement or prosecutorial agencies or the judiciary Used to share investigation/prosecutorial findings which are required to meet evidentiary standards and tends to include more specific operational and personal data types, such as communications data, metadata and geo-location data Predominantly public-public information flows	LEAs Prosecution Judiciary
International secure networks	Usually, operationalised and maintained by an international body (e.g. Egmont) Used mainly for cross-border strategic and/or operational information sharing Predominantly public-public information flows across multiple jurisdictions	LEAs Supervisors FIU

[8] Lesotho, Liberia, Myanmar, North Macedonia, Portugal and Spain.

Institution-specific protected systems	Usually, operationalised and maintained by supervisory authorities Used by supervisors to collect and share information which is specific and unique to their respective institutional design and functions (e.g. central bank supervisory portals, securities regulator systems) Multi-dimensional information flows (i.e. public-private and private-public) Platforms are generally encrypted, auditable and with access restricted to the relevant stakeholders	Supervisors Reporting entities, including FIs/DNFBPs/VASPs

Source: Survey responses.

Public-Private Partnerships as an enhanced mechanism of information sharing

Definitions, key characteristics and principles of Public-Private Partnerships

21. The FATF Recommendations broadly require information sharing in several instances. PPPs are not required by the Standards, but MERs and prior FATF studies show they are a comprehensive way of exchanging information more quickly and efficiently, and are generally understood as an enhanced form of collaboration between a public and a private body, established on a voluntary basis. Although there is not one definitive, universal definition of PPPs, the FATF's Guidance on private sector information sharing[9], and then the FATF's report on Partnering in the fight against financial crime, defined them as mechanisms which facilitate information sharing between public and private sector stakeholders in a manner that increases the effectiveness of AML/CFT/CPF measures by facilitating a more comprehensive overview of financial transactions and customers' behaviours.[10]

22. Another study by the Future of Financial Information Sharing initiative[11] referred to PPPs as mechanisms which provide regularly convened, dynamic public–private dialogue on financial crime threats, based on shared and agreed objectives and priorities. The working definition of PPPs (Box 1) being used in this document builds on the above definitions.

23. Based on survey responses and previous work, these are some of the characteristics PPPs exhibit, to varied extents, depending on the purpose and nature of the relevant PPP:

- **Mutual Benefit and added value.** PPPs must ensure both public and private sectors benefit from the outcomes of the activity taking place within the PPP, including through meaningful and reciprocal information exchange. Effective cooperation requires two-way communication, with all parties both contributing relevant information and receiving actionable feedback, strategic insights or operational value in return. PPPs should also add to what can already be shared rather than being created for its own sake.
- **Joint activity.** PPPs should aim to identify, reduce, mitigate or disrupt threat activity or eliminate vulnerabilities through resilience or education.
- **An enabling framework.** A framework or enabling set of arrangements aligned with FATF Standards (e.g. efforts to improve STRs), international recommendations and best practices that defines mandate, scope and objectives is necessary, as well a high-level political commitment that guarantees the necessary resources for PPP performance (see separate section on Governance and budget for further details).
- **Metrics.** Performance indicators should be incorporated to measure impact as they are needed for tracking the effectiveness of a PPP.

[9] FATF (2017), Guidance on private sector information sharing, FATF, Paris, available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private-Sector-Information-Sharing.pdf.coredownload.pdf.

[10] FATF (2022), Partnering in the fight against financial crime, FATF, Paris, available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.

[11] RUSI (2017), The Role of Financial Information-Sharing Partnerships in the Disruption of Crime, available at: https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_report_-_oct_2017_web_1.pdf.

- **Legal Basis for Exchange.** Information-sharing requires explicit legal authority, identification of competent entities, and clear legal rules specifying what information may be shared and under what conditions.
- **Data Protection and Confidentiality.** All information exchanges must comply with data protection and privacy standards, including lawful processing, retention limits, anonymisation/minimisation, and administrative, technical, and contractual safeguards.
- **Differentiated Channels and Need-to-Know Access.** Information flows must be segregated by purpose (e.g. strategic vs. operational) with access levels granted according to role and strict need-to-know criteria.
- **Duties, Responsibility and Accountability.** Participants must have reciprocal obligations to provide relevant information, limit use to authorised purposes, notify breaches, and accept proportional liability for non-compliance.
- **Risk Management and Risk-Based Approach.** Participants must conduct periodic risk assessments, align activity with national priorities, and adapt dynamically to emerging threats and changing risk profiles.
- **Inclusive Governance and Representation.** Governance structures should ensure representation of relevant public authorities and trusted private sector entities (FIs, DNFBPs, VASPs, civil society and other entities and businesses where appropriate), with clear admission and dispute-resolution rules. This can include entities offering technology or communications services (including, social media, instant messaging and streaming platforms) as well as NPOs and academia depending on each jurisdiction's needs and context.
- **Operational Capacity and Cybersecurity.** Participants and the platform used for exchanging information must meet minimum technical and operational standards (encryption, authentication, access and security), and maintain training and analytic resources to respond effectively.
- **Interoperability and Standardisation.** Information exchange must use common formats to ensure efficient, auditable, and machine-readable sharing across entities.

Purposes of Public Private Partnerships

24. PPPs improve the ability of competent authorities and the private sector to detect, analyse and disrupt financial crime activity at speed and scale. They create structured environments, often secure and encrypted, where authorities share priority threats, early-stage intelligence gaps, relevant patterns of behaviour and targeted operational guidance. In practice, this enables private entities to conduct targeted analysis of customer and transactional data, respond to financial analysis requests and financial monitoring requests, and identify activity linked to ongoing criminal or national-security investigations. In some cases, these arrangements include targeted or tactical mechanisms designed to support timely and coordinated action in parallel by law enforcement and reporting entities.

25. Going beyond regular information sharing already expected and provided for by FATF Standards as part of AML/CFT Regimes, PPPs can also serve the operational purpose of building trust and confidence (through regular engagement) to secure more efficient and faster AML/CFT/CPF outcomes through deeper, different types of engagement between the public

and private sector. See examples from France, Indonesia and Saudi Arabia below, which show different forms of how such engagement can materialise.

Box 2. Protecting your country through an Advanced Tech PPP platform

SIPENDAR (Sistem Informasi Terduga Pendanaan Terorisme) is a PPP online secure platform established by Indonesia's FIU (PPATK) in 2021 to detect and immediately respond to terrorism activities and its financing. SIPENDAR mainly exchanges three types of information, which are (1) typologies, current trends, and strategic analysis on TF (confidential version); (2) watchlist on TF activities; and (3) spontaneous and mutual request platform.

SIPENDAR can be accessed by TF related agencies (i.e., PPATK, National Police (POLRI), National Terrorism Body (BNPT), State Intelligence Agency (BIN), Customs, and Immigration) and by the private sector once cleared through the intelligence vetting system of dedicated officers prior to accessing SIPENDAR. SIPENDAR has (1) developed a watchlist on TF activities which combines machine learning and human intelligence and disseminates the list to the private sector, also requiring private sector to enrich information on targeted individuals and entities under the watchlist and report it to PPATK in a timely manner; and (2) supported immediate responses to any terrorism incident, including potential incidents of terrorism less than 24 hours after the information has been announced by competent authorities.

How the PPP made a difference

- The PPP helped with the early detection of incoming and outgoing virtual assets related to ISIS, which led to an immediate response by competent authorities, including immediate information exchange with foreign counterparts.
- The PPP's tech platform reduces bureaucracy on domestic coordination and exchange of information. The dissemination of information between public and private sector is faster and more effective.
- The development of watchlists on TF is helping the private sector to detect and report TF STRs.
- The timely information enables both the public or private sector to provide a response in an immediate manner, and as a result can produce early detection that can prevent terrorism activities across competent authorities.

Source: Indonesia

Box 3. "CTF committee" – a French PPP dedicated to counter terrorism financing

Financial information, particularly that provided by FIs, is a key source of intelligence which, after collection, analysis, enhancement, exploitation and cross-

checking by Tracfin, helps to detect terrorist networks, prevent terrorist financing campaign and terrorist actions.

Tracfin set up in 2019 a PPP dedicated to CFT – Comité LFT - composed of 16 financial institutions: 7 banks, 6 payment institutions, 2 Virtual Asset Service Providers, and 1 crowdfunding company. This committee, co-chaired by two members of the private sector, has introduced a new form of PPP, based on trust and confidentiality, in compliance with French laws.

Meeting three to four times a year, this committee allows participants to be informed, to share, to brainstorm and to exchange views on new threats, trends and typologies linked to CFT. The topics discussed are varied, from the use of cryptocurrency by terrorist groups to identifying good/bad practices in terms of STRs in the field of terrorism financing. Tracfin or the Committee members can suggest topics for discussion. Partners such as intelligence services/administrations such as the French Treasury or the national anti-terrorist prosecutor's office (PNAT) are also regularly involved.

Source: Tracfin (French FIU)

Box 4. Trust that leads to outcomes

Action was initially triggered in the context of Saudi Arabia's informal PPP by a high volume of international transactions identified by a bank as unrelated to the purpose reported by the customer of that bank (e.g. corporate main activity being sale of phones and other technology related goods but the transactions being made to a biochemical company).

Prior to the PPP collaboration between the public and private sector information sharing and partnerships were slower. The PPP helped in expediting the process and provided a clearer way to tackle AML/CFT risks. As a result of this bank's alert, the company's assets were frozen and a person is currently being prosecuted. The case was used in a workshop after which other banks started to apply enhanced due diligence to companies that share a similar nature of business.

How the PPP made a difference

- the PPP to expedite the communication between the public and private sectors as a result of trusted, established relationships and accelerated the timelines by removing the bureaucracy between the public and private sectors.

Source: Saudi Arabia

26. Authorities can use PPPs to issue timely alerts to reporting entities, helping them identify relevant activity and improving the usefulness of STRs. Through PPPs, institutions receive early warning about new typologies, for example on fraud schemes and methods, supporting proactive mitigation and contributing directly to better AML/CFT/CPF outcomes. In this sense PPPs and private-to-private partnerships need to be considered strategically together. For example, for fraud, while private-to-private sector information sharing can help with prevention, PPPs can focus on investigation of complex criminal networks.[12]

27. PPPs provide a safe environment for data mining, operational analysis and scanning by the public and private sector. This model helps fill intelligence gaps while respecting national legal frameworks and confidentiality obligations and may also facilitate structured feedback loops that enhance both tactical responsiveness and longer-term strategic financial intelligence gathering and law enforcement actions.

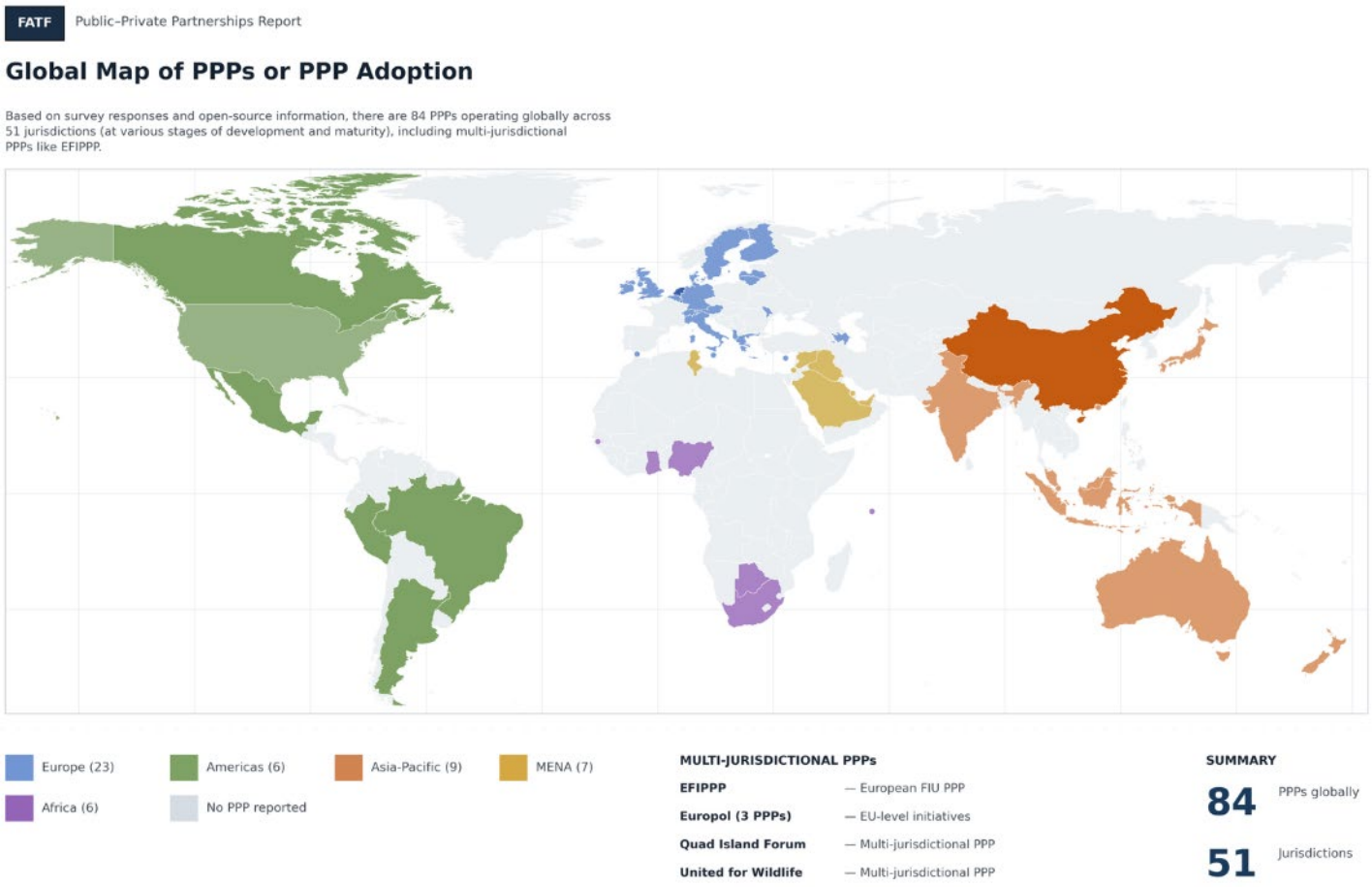
Mapping and diversity of global Public-Private Partnership implementation

28. Based on survey responses and open source information[13], there are at least 84 PPPs operating globally (at various stages of development and maturity) including transnational PPPs like EFIPPP (see below). Although efforts were made to capture as many PPPs as possible, the mapping may not cover the entire universe of existing PPPs globally, in part due to the timing of this survey, which may not capture those developed after October 2025. Fifty-two survey respondents have at least one domestic PPP, with eighteen declaring more than one domestic PPP within their jurisdiction.

[12] A survey of collaborative analytics platforms to tackle fraud (FFIS, May 2026), available at: https://www.future-fis.com/fraudplatforms.html. See also UNODOC Fraud toolkit on PPPs against organised fraud (UNODOC, May 2026), available at: https://www.unodc.org/res/organized-crime/GFS/publications/UNODC_PublicPrivate_Partnership_Toolkit_Against_Organized_Fraud_EN.pdf.

[13] For example, the Technical Annex to the European Survey of PPPs developed by EFIPPP documented success cases extensively on how PPPs have contributed to fill intelligence gaps, from increasing STRs to concrete enforcement action. Examples include both results from +10 years' experience PPPs (e.g. the UK's JMLIT Joint Money Laundering Intelligence Taskforce – JMLIT+) and more recent PPPs (e.g. See case of Latvia's PPP).

Figure 1. Global Map of Public-Private Partnerships or Public-Private Partnership Adoption



Note 1: Colours represent different jurisdictions in the world where PPPs exist.
Note 2: Disclaimer This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.
Source: Survey responses.

29. There are different types, structure, participants and organisation of PPPs. The UN CTED's Analytical Brief (which maps PPPs on terrorist financing) notes that there is wide diversity in the PPP landscape, with most PPPs having a broad scope.

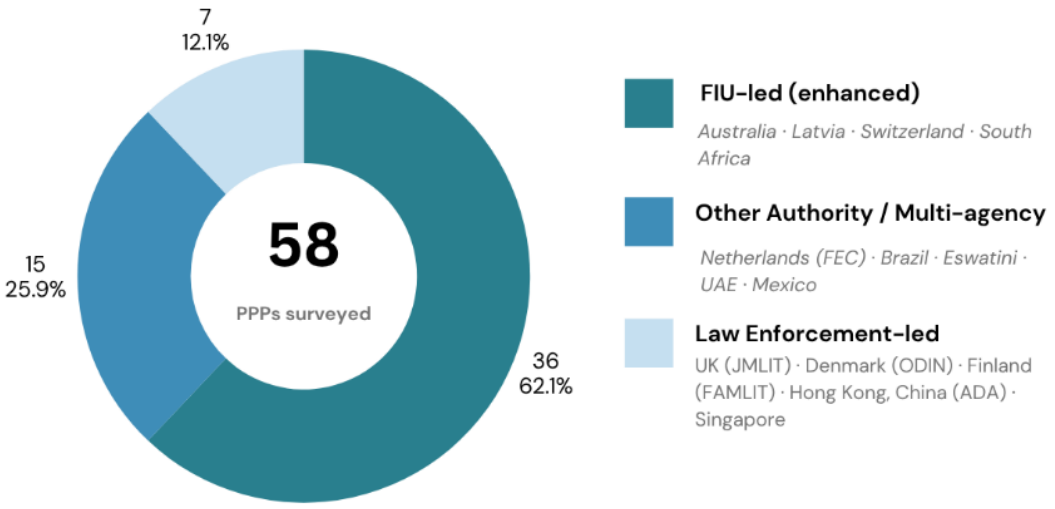
Timespan

30. Whilst most identified PPPs are continuous permanent features of a jurisdiction's AML/CFT framework, some mechanisms classified by their governing authority as a PPP, are dynamic time-bound collaborations established for a specific short-term purpose. Others feature time-bound sub-groups or functions within the broader PPP that focus on targeted activity over a limited time or activity focused period.

Leadership

31. PPPs can be led by a range of stakeholders. As illustrated below, the majority of domestic PPPs are coordinated and/or hosted by Financial Intelligence Units (FIU)[14] but they can also be led by other agencies.[15]

Figure 2. Public-Private Partnership Leadership



Source: Survey responses.

32. Eight PPPs are law enforcement led, although they comprise multi-agency public sector participants:

- Denmark's Operational Danish Intelligence Network (ODIN) led by the National Special Crime Unit of the Danish Police.
- Finland's Anti-Money Laundering Intelligence Taskforce (FAMLIT) led by the Financial Intelligence Unit of the National Bureau of Investigation.
- Hong Kong, China's Anti-Deception Alliance (ADA) comprising ten participating banks, who work with the Hong Kong Police Force Anti-Deception Coordination Centre (ADCC) officers. Some licensed securities firms have also established protocol with the ADCC to facilitate the 24/7 stop payment mechanism to expedite interception and recovery of crime proceeds. The Virtual Asset Intelligence Taskforce (VAIT), a collaboration among LEAs, regulatory bodies and key VASPs. The Financial Intelligence Evaluation Sharing Tool

[14] The Egmont Group's Information Exchange Working Group (IEWG) is currently undertaking a project to identify, document and share international best practice in public-private partnerships for AML/CFT. Drawing on global models, Egmont, FATF and industry guidance, the project aims to develop a practical toolkit – including templates, legal gateways, and performance metrics, to help FIUs and private-sector partners establish and enhance effective PPPs. The report that will be prepared will also provide a practical guidance for design, governance and operationalisation of PPPs in the fast-changing ML/FT context. The project is in its mapping phase, and the project leads are FINTRAC, FIU El Salvador and FIU Bermuda.
[15] In some countries, FIUs lead other information sharing mechanisms but these may not be labelled as PPPs.

(FINEST) financial intelligence sharing platform is administered by the HKPF in partnership with the Hong Kong Monetary Authority and the Hong Kong Association of Banks.

- Malaysia's NSRC (National Scam Response Centre, NSRC) operates under the leadership of the Royal Malaysia Police (RMP) and the supervision of the Ministry of Home Affairs (MOHA). The NSRC brings together the financial regulator (Bank Negara Malaysia), the telecommunications regulator (Malaysian Communications and Multimedia Commission), the National Anti-Financial Crime Centre, banks and telecommunication providers to share resources and information for rapid inter-agency action to combat scams.
- New Zealand's NZ-FCPN (New Zealand Financial Crime Prevention Network) is chaired by the New Zealand Police FIU.
- Singapore's ACIP (AML/CFT Industry Partnership) is jointly coordinated by the Commercial Affairs Department (CAD) of the Singapore Police Force (SPF) and the Monetary Authority of Singapore (MAS). SPF also operates Singapore's Anti-Scam Centre (ASC) which was set up by the SPF to serve as the Police's nerve centre for investigating scam-related crimes.
- The United States' CI-FIRST (Feedback in Response to Strategic Threats) establishes ongoing engagement between the Internal Revenue Services Criminal Investigation (IRS-CI) and financial institutions, led by IRS-CI.
- The UK's Joint Money Laundering Intelligence Taskforce (JMLIT+) which sits alongside the UK Financial Intelligence Unit (UKFIU) Engagement function, and is led by the National Economic Crime Centre, a command within the UK's National Crime Agency, and the National Lead Force, within City of London Police, that comprises the PPPs of the Dedicated Card & Payment Crime Unit (DCPCU), Police Intellectual Property Crime Unit (PIPCU) and the Insurance Fraud Enforcement Department (IFED).

33. Fifteen PPPs are coordinated by other authorities, including some with a narrower information sharing purpose such as Brazil's Coordenação de Repressão à Corrupção (Coordination for the Repression of Corruption) concerned with combating sports match-fixing. While the UK's FIN-NET (Financial Crime Information Network) with a broad remit to combat fraud and financial crime through its domestic and international public and private sector participants, operates under the UK's financial services regulator.

34. PPPs can also be co-led by the public and private sectors (see example below).

Box 5. Canada's Diverse Public-Private Partnership Models for AML/CFT

In Canada, some PPPs are co-led by both the FIU (FINTRAC) and the private sector. This ensures strong mutual participation by, and benefit for, the private sector. With the purpose of creating a channel of communication from the private sphere to the public. This model has allowed FINTRAC to contribute to a process that has resulted in proactive financial intelligence to law enforcement based on information received from the private sector. It has increased the speed and the ability of the Canadian regime to proactively target more sophisticated crimes, without requiring changes to Canada's legislation. In turn, by sharing information, regulated entities have additional information and data to support their ability to detect suspicious transactions, accurately assess risks, inform risk-based measures and support compliance with their obligations, including reporting suspicious transaction to FINTRAC.

The Canada Revenue Agency leads the Canadian Financial Partnership (CFP), a domestic PPP that brings together major financial institutions, industry representatives, and federal partners to address tax evasion and ML risks. Through regular engagement, including virtual discussions and annual meetings, the CFP enables strategic-level information sharing, joint threat assessments, and the development of typologies, while fostering strong networks across public and private sectors. This collaborative model enhances Canada's ability to identify and respond to financial crime threats and contributes to broader international efforts.

Canada's Advisory Committee on Money Laundering and Terrorist Financing (ACMLTF) is a high-level discussion forum to address emerging issues and provide advice on Canada's AML/CFT Regime both within a domestic context and in support of international AML/CFT developments. ACMLTF consists of public sector representatives from the Department of Finance, FINTRAC, the Office of the Superintendent of Financial Institutions (OSFI), and Public Safety Canada. Private sector participants are drawn from sectors including financial entities, life insurance companies, securities dealers, money service businesses, virtual currency dealers, accountants, the notarial profession, the real estate sector, casinos, dealers in precious metals and stones, and home builders.

On February 19, 2025, the Government of Canada convened the first working meeting of the new Integrated Money Laundering Intelligence Partnership (IMLIP). This new public-private partnership supports the permissible sharing of money laundering and organised crime intelligence between law enforcement and Canada's domestic systemically important banks (DSIBs), and bolsters Canada's response to organised crime and high-end money laundering schemes, including related to fentanyl trafficking. The partnership will also help facilitate strong working relationships between law enforcement agencies and the financial services sector, to establish a greater understanding of money laundering threats that face Canada. The Government has announced its intention to amend the Proceeds of Crime (Money Laundering) and Terrorist Financing Act with related amendments to the Personal Information Protection and Electronic Documents Act to clarify public to private information sharing provisions to help better detect and deter money laundering and support the recently created IMLIP between banks and law enforcement.

Source: Canada

Composition

35. 22% (18) of PPPs are considered a multi-agency PPP. Most notably the Netherlands' PPPs which function under the Financial Expertise Centre (FEC), a cooperative association of the Netherlands Authority for the Financial Markets (AFM), General Intelligence and Security Service, Tax and Customs Administration, De Nederlandsche Bank, Fiscal Intelligence and Information Service and Economic Investigation Service, Public Prosecution Service, the Netherlands Police and FIU-the Netherlands.

36. Eight survey respondents (Angola, Bahrain, Benin, Eswatini, the Marshall Islands, Saudi Arabia, Syria and the United States) shared that their FIU-led PPPs hold regular in-person and virtual meetings with, and/or issue sector-specific guidelines to their obliged entities, which could be considered a form of PPP as this engagement extends beyond what FIUs may usually undertake in engagement with the private sector.

Box 6. Eswatini AML/CFT Committees (multi-agency PPP) for information sharing

Eswatini has an AML/CFT Task Force which comprises a Council and a Technical Committee tasked with the development of the country's AML/CFT National strategy plan and ensures implementation and approval among other functions. The technical committee includes both the public and private sector. Public sector representatives include the Ministry of Finance, FIU, AML/CFT supervisors, self-regulatory bodies, law enforcement agencies, Director of Public Prosecutions and Attorney General's office. The private sector comprises Bankers Association, Law Society and the Eswatini Institute of Accountants. This committee meets on a monthly basis and facilitates AML/CFT information sharing among stakeholders.

Source: Eswatini

Box 7. Latvia Cooperation and Coordination Group (CCG) – Rapid, Flexible, Case Support

Latvia's CCG was established as a public-private (and public-public) partnership in 2018 with an agile and flexible model. CCG meetings can be convened immediately, enabling fast operational or strategic coordination between the FIU, law enforcement, prosecutors, supervisors and reporting entities. Meeting attendees vary depending on the need and purpose of the meeting.

Successful outcomes include:

- Increase in number of STRs and contribution to strategic products.
- Complex cases discussed with LEAs and reporting entities to support ways forward.
- Case 1: In 2021 the FIU, within the CCG framework, gathered experts from the FIU, prosecutor office (PO), Corruption Prevention and Combating Bureau (CPCB) as well as four largest Latvian credit institutions. The experts developed corruption and ML indicators and added to them relevant case study material. The material is to be used by credit institutions (as well as other reporting entities and LEAs) in detecting and investigating corruption. The document includes a list of red flag indicators for transactions which may be corruption related and also other factors that may lead to a suspicion of corruption. As a result, a study was finalised and then published on the FIU's webpage. In the aftermath of the publishing of the study, there was a significant increase in STRs tied to the predicate of corruption (67 in 2021; 104 in 2022).
- Case 2: The State Police initiated an investigation on trafficking in human beings in 2020. To ensure a swift and co-ordinated response, a CCG meeting was immediately convened. State Police informed participants of the circumstances of the case and planned activities, while ensuring its confidentiality. The FIU issued orders via the secure channel of goAML to FIs (providing each FI only with information concerning their respective customers) to monitor transactions on the accounts of the persons suspected of the crime and rapid co-operation with foreign FIUs led to temporary freezing of funds abroad ahead of MLA. As a result, significant assets were seized and frozen. In May 2024, a criminal case indicting 10 natural persons and one legal person for trafficking in human beings and aggravated ML was brought before the Economic Crime Court where trial is underway.

Latvia highlights having a clear robust legal framework and an adaptable model as key factors of success.

Source: Latvia

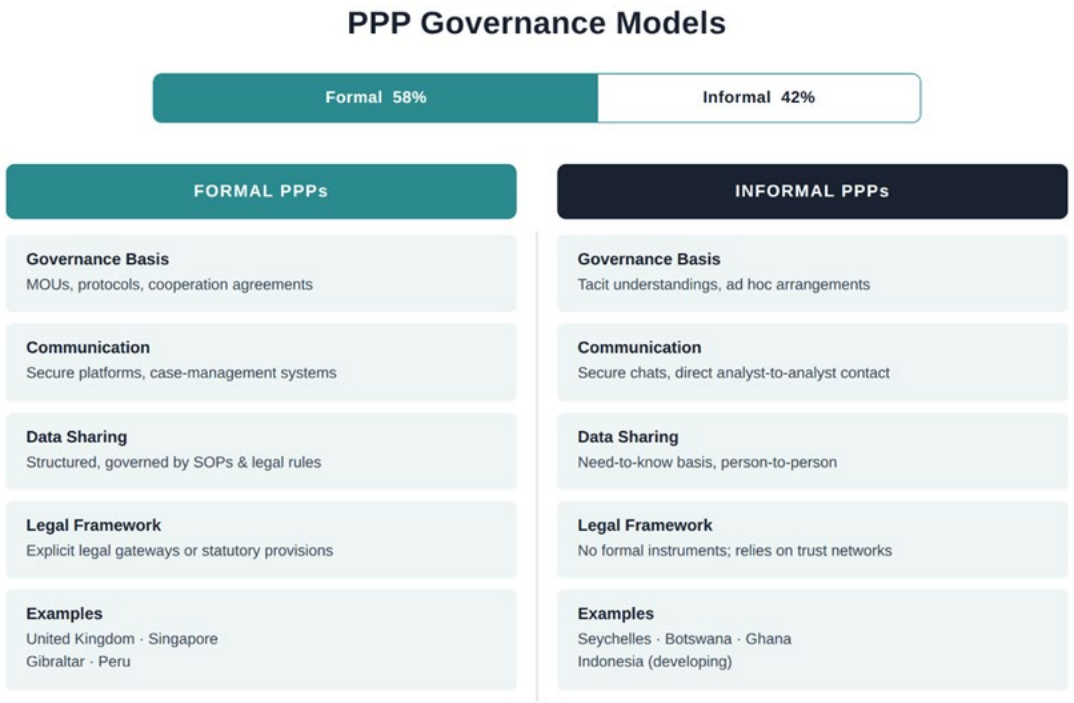
Governance structures to support Public- Private Partnerships

37. PPP operations require high-level political commitment, administration support, as well as support from the private sector, especially in relation to data sharing. Budgetary allocations may also be needed to support them; one quarter of responses noted they have specific budget allocations (including co-funding by different members of the PPP) which is encouraging.

38. PPP governance refers to the set of enabling arrangements that defines the mandate, scope, and objectives of the partnership in alignment with international standards, particularly the FATF Recommendations on information sharing.[16] By setting explicit objectives from the outset, governance frameworks provide the legal, policy and/or operational foundation that allows PPPs to function effectively within the limits of national legislation and also contribute to transparency (e.g. as to what can and cannot be shared).

39. PPPs can have formal or informal structures and governance as shown below. There are also PPPs that began informally but have evolved into some level of formalisation based on policy-led arrangements. The range of structures applied reflects the needs and the legal and institutional context of various jurisdictions.

Figure 3. PPP Governance Models



Source: Survey responses

[16] Recommendations 2, 20, 29, 31 and interpretative notes on information sharing.

Formal PPPs

40. Over half of respondents (58%) indicated they have a formalised model of PPP based on institutionalised governance frameworks such as:

- MOUs, protocols, or cooperation agreements
- internal Standard Operating Procedures and governance frameworks
- secure communication systems or case-management platforms
- sector-specific laws/regulations that define roles and boundaries.

41. Even where jurisdictions have formal PPPs, informal sharing is also permitted and is often essential for early warning or pre-STR insights.

42. Some features of formal PPPs include:

- **Format:** PPPs organise their work in a variety of ways, with frequency and meeting type varying in accordance with their governance and/or their operational nature. PPP meetings may be held at varying intervals: quarterly strategic meetings, monthly or bi-monthly operational working groups, or in some instances, even daily or near-real-time exchanges.
- For example, in long established formal PPPs, such as those in Singapore and South Africa, meetings happen about 3 or 4 times a year. This is also the case for the UKFIU's 10 facilitated PPP working groups who meet 3-4 times per year, under agreed Terms of Reference, and which include participants from non-banking sectors such as insurance, accountancy, art house auctioneers and real estate.
- Some operational PPPs such as Australia (Fintel Alliance) and UK (JMLIT+) have multiple working group meetings with daily communication, monthly tactical meetings, daily information inputs, and continuous sharing of information. Latvia has a joint operational centre where FIU Latvia analysts and LEA officers work together on the most complex and high-priority criminal cases, ensuring rapid information exchange and coordinated operational action (OpCEN). South Africa (expert and tactical groups) allows for joint operational meetings allowing real-time case collaboration. In the Netherlands, their operational groups meet twice weekly on cases of high frequency. Other important features of formal PPPs include:
    - **Clear legal basis:** The most common barrier to effective information sharing is legal uncertainty. PPPs function best when legislation clearly defines roles, mandates and permissible data-sharing pathways, not prohibitions.
    - **Safe harbour protections:** Advanced PPPs such as Singapore's COSMIC, Gibraltar's FLINT, UK's JMLIT+, and several EU initiatives include safe-harbour clauses that protect private institutions acting in good faith from liability under secrecy or data protection rules.
    - **Formal documentation:** High-performing PPPs use MoUs, Terms of Reference and written procedures that set out confidentiality safeguards, escalation routes, governance structures and limits on data use.
    - **Data protection alignment:** Despite privacy rules being widely cited as constraints, roughly three-quarters of jurisdictions report having safeguards—

encryption, access controls, audit trails—that enable sensitive information to flow lawfully.

43. Strong governance ensures predictability, reduces institutional risk aversion and builds the confidence needed for operational collaboration.

Informal PPPs

44. Informal PPPs operate without MOUs, formal channels or data-sharing restrictions. Operating within each jurisdiction's legal environment, informal PPPs rely on flexible arrangements that allow agencies to collaborate effectively without structured governance, administrative support, or designated data sharing frameworks. These arrangements are characterised by tacit understandings between agencies, ad hoc consultations, person-to-person contacts and coordination groups without formal legal instruments.

45. Informal PPPs rely on trust networks, and operate via working groups, industry roundtables, secure chats/briefings and ad hoc calls with FIU/LEA, committees and face-to-face meetings where parties can share challenges and collectively identify ways of tackling them. Botswana, Eswatini, Ghana, Indonesia and Seychelles are currently developing informal sharing and expect their PPPs to expand into controlled informal interactions. Communications are conducted through continuous, informal communication channels, messaging-style secure chats, direct analyst-to-analyst contact, or embedded liaison officers.

Membership

46. The majority of PPPs tend to include domestic FIs in addition to the primary operator of the PPP. Others include foreign FIs, their central bank, regulators and supervisors, and/or participants from other government departments, such as customs, intellectual property authorities, the judiciary, tax, and entities from the wider financial sector, such as insurance, investment, securities, trade bodies, VASPs and third-party payment service providers. A smaller number of PPPs include participants from other industry sectors, including accountancy, gambling, eGaming, legal, online marketplaces, real estate, social media, technology, telecommunications as well as academia and NPOs/civil society. Selection for membership in a PPP is typically made by the PPP lead organisation and driven by a number of factors, including:

- Market share
- Risk appetite
- Relevance/exposure to emerging threats
- Regulatory status
- Ability to contribute to the objectives of the PPP
- Willingness, ability and extent to which the necessary information and/or expertise relevant to the threats and objectives is provided.

47. Membership in a PPP may require consent via MOUs or confidential undertakings, accompanied in some cases by orientation on the access, use and handling of information and data systems. Australia, Singapore, the US and the UK's JMLIT+ require the security vetting of members. Peru, Botswana, Gibraltar and the UK have specific procedures or clauses in MOUs or other PPP policies for the removal of membership in certain circumstances.

48. PPPs may expand to include other industries and services as needs and regulatory environment evolve. For example:

- with regulatory changes expected in July 2026, Australia reported it will consider partnering with real estate professionals, dealers in precious stones and metals dealers (DPMS), legal practitioners and trust and company services providers (TCSPs).
- Cyprus and Gibraltar models are considering including virtual asset service providers in their PPPs.
- In the UAE, the PPP framework is expected to expand to include additional competent authorities and sectors, including VASPs, cybersecurity, environmental protection, and gaming regulation.
- In Austria, PPPs exist in the financial sector (banks and VASPs/CASPs), in the legal professions, for real estate agents, DPMS and TCSPs according to the trade act, and for NPOs. A further PPP on the topic of gambling is planned, as is a public-public partnership initiative of the FIU with the law enforcement authorities (investigators from various investigative fields) and the judiciary.

49. FATF's Comprehensive Overview of Terrorist Financing Risks Report and the Non-binding guiding principles on preventing, detecting and disrupting the use of new and emerging financial technologies for terrorist purposes (the Algeria Guiding Principles) also encourage expanding engagement with sectors that currently fall outside regulated entities, particularly digital and online platforms (e.g. instant messaging apps, online gaming and entertainment platforms, crowdfunding sites, and social media channels). This is to foster mutual understanding of sector-specific threats, and encourage integration of TF and other risk mitigation strategies into product design. In this context, public and private sector actors can collaborate to test market innovations, including through regulatory sandboxes, to jointly identify risks, build a shared understanding of emerging threats, and pilot proportionate regulatory responses. Such collaboration can be supported by structured dialogue with relevant financial technology and digital platform providers to strengthen operational and tactical analysis.

50. Diverse membership is likely to derive an enriched information dividend, but such value needs to be balanced against the resources needed to manage the additional management responsibilities they entail. To help with this, there is existing evidence that the use of technology, such as remote/virtual participation, can facilitate PPP participation.

Types of information shared

51. Information shared through PPPs encompasses three broad categories, which depend on their purpose: (i) Strategic information; (ii) Operational information; and (iii) Information on targets or person(s) of interest.

Box 8. Types and modalities of partnerships depending on type of information shared

Strategic information sharing partnership refers to the exchange of aggregated, contextual, and risk-based patterns between public and private sector to enhance the common understanding of AML/CFT/CPF risks. Unlike operational or case-specific exchanges, strategic sharing does not focus on identifiable individuals or transactions, but rather on trends, typologies (e.g. could be co-developed in/within PPP), vulnerabilities, and emerging threats observed across sectors or jurisdictions. This may include analyses of evolving criminal methodologies, sectoral risk assessments, or anonymised patterns of suspicious activity aimed to fostering a shared understanding of the risk landscape. Strategic information sharing supports the development of more effective risk-based approaches, strengthens preventive controls, and enables both authorities and reporting entities to better anticipate and mitigate risks, while remaining consistent with applicable data protection and confidentiality requirements. Safe harbour provisions can encourage PPP participants to share information, enhancing the effectiveness of combatting illicit finance.

Operational information sharing partnerships enable the exchange of timely, actionable, and often case-related information on incidents, actors, entities, and their associated financial activities. These arrangements typically involve the sharing of more sensitive information—including, where permitted, personal, financial, and suspect-related data—which may support financial intelligence development and, in certain cases, contribute to investigative processes. In this context, the private sector moves beyond a solely compliance-oriented role to act as a contributor to the detection and analysis of potential illicit activity. Operational exchanges help reporting entities enhance the effectiveness of customer due diligence measures, improve transaction monitoring, and identify higher-risk customers and their patterns of activity. Operational PPPs may vary in structure: some involve a broad range of financial institutions, while others adopt a more targeted, threat-based and capability-driven approach, focusing on key sectors or institutions that are particularly exposed or best positioned to contribute to specific risk areas. Operational exchanges help reporting entities enhance the effectiveness of customer due diligence measures, improve transaction monitoring, and identify higher-risk customers and their patterns of activity. Operational PPPs may vary in structure: some involve a broad range of financial institutions, while others adopt a more targeted, threat-based and capability-driven approach, focusing on key sectors or institutions that are particularly exposed or best positioned to contribute to specific risk areas. Given the sensitivity and potential use of this information, operational information sharing within PPPs should be grounded in clear legal bases and subject to appropriate safeguards, including confidentiality, data protection, and, where applicable, judicial or regulatory controls. In particular, where information is intended for use in investigative or prosecutorial processes, formal information-sharing mechanisms established under domestic legal frameworks remain the appropriate channel. Accordingly, operational PPPs should be understood as complementary tools that enhance the timeliness and quality of financial intelligence, without replacing formal procedures required for evidentiary or judicial purposes.

Hybrid partnerships: PPPs that share both strategic and operational information.

Modalities of partnerships

- Dedicated co-located workspaces with access restricted to nominated personnel or key participants only, enabling real-time collaboration in cases or operations
- Dedicated communication platforms for information exchange
- Cooperation on a more targeted basis (incl. bilateral protocols on information exchange)
- Domestic information sharing
- Supranational level; more permanent structure
- FSRB regional initiatives on public-private cooperation

Strategic information

52. Most PPPs share strategic information. Because it is less legally complex, strategic sharing often also acts as a starting point and trust-building mechanism that helps create a shared understanding of risks (See example of Peru below). Jurisdictions can then move to more sensitive operational exchanges that can materially enhance effectiveness in investigating ML/TF. The key categories of strategic information include:

- **Typologies and Red Flags:** These are widely disseminated to help institutions identify suspicious patterns. This category is reported by over 75% of jurisdictions.
- **Risk Trends and Emerging Threats:** Many jurisdictions share sectoral risk assessments and thematic findings on evolving threats such as virtual assets and cyber-enabled crime. This proactive approach of sharing helps institutions anticipate and mitigate emerging risks.
- **Beneficial Ownership Information:** Approximately one-third of participating delegations provide access to beneficial ownership data, often through open sources or registries, to support transparency and due diligence.
- **Activity Reports and Feedback on STRs:** Many FIUs share annual reports, feedback on STRs, and sectoral vulnerability assessments. These exchanges improve the quality of reporting and strengthen compliance frameworks.

Box 9. Strategic information sharing PPPs

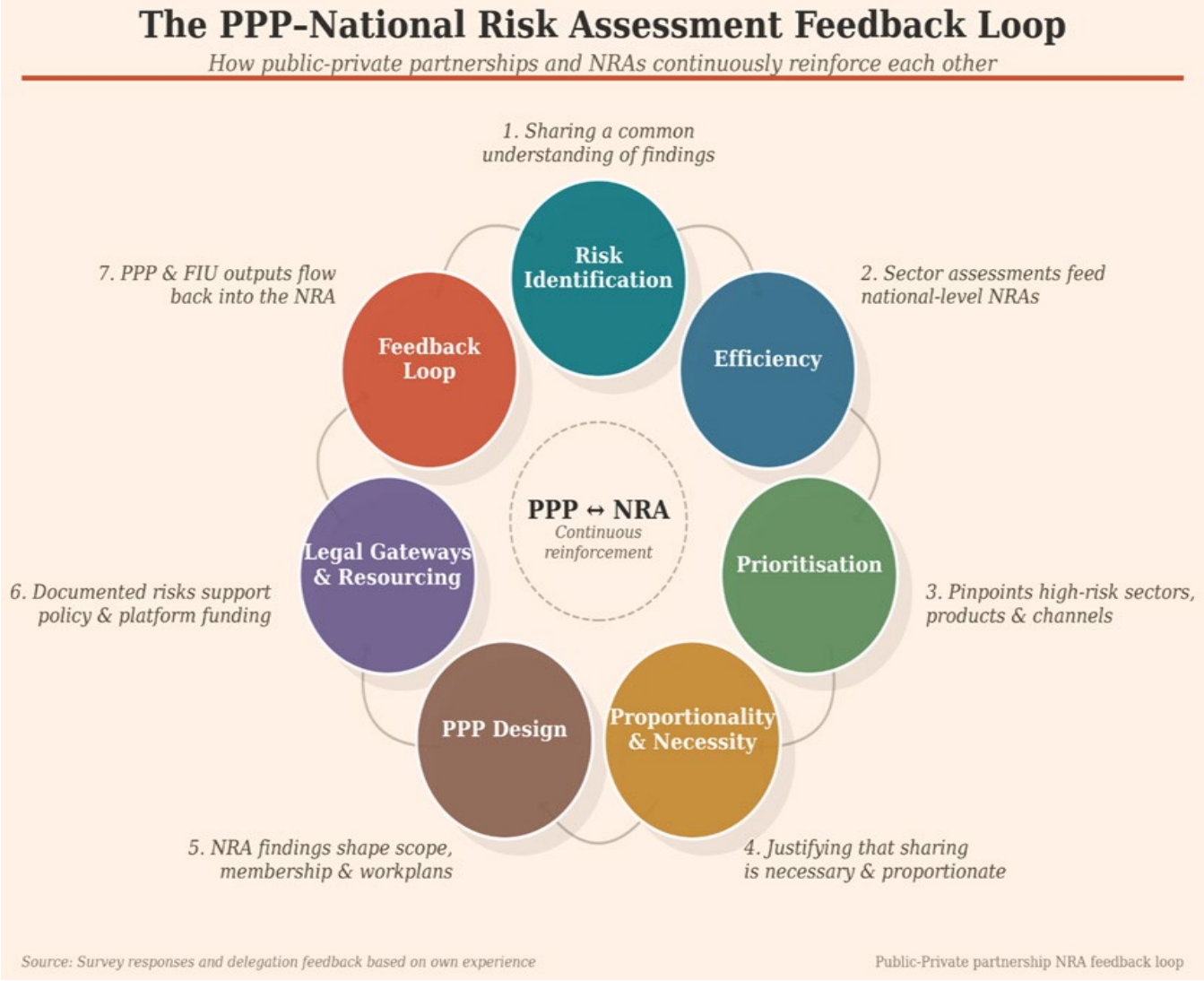
The Public-Private Financial Information Sharing Mechanism (MEPIF) was established in Peru in September 2024 as a permanent, specialised technical arrangement without legal personality. It is designed to enable the **secure, effective, and collaborative exchange of strategic and operational information** between public and private sector participants.

With a view to building trust and consolidating effective working arrangements among its members, MEPIF initially prioritised the exchange of **strategic information**, such as statistics, trends, and patterns. In this context, members agreed by consensus that the first outputs would be a **Typologies Catalogue** and a **Red Flags Guide** focusing on **illicit financial flows linked to human trafficking**. This decision was driven, inter alia, by the national context characterised by the growing presence of organised crime and its operational and financial convergence with human trafficking; the **low level of enforcement outcomes targeting illicit financial flows derived from this crime**; and the need to bring together previously fragmented efforts by private-sector stakeholders to improve understanding of the **economic and financial dimensions of human trafficking**. The aim of the initiative is to increase the volume and quality of Suspicious Transaction Reports (STRs) related to human trafficking, to strengthen the **preventive and detection capabilities of the AML/CFT framework** in line with the risks identified.

Source: Peru

53. One important use of PPPs is their contribution to national level risk assessments (NRAs) and other assessments and strategies, where there is a constant loop as shown in figure 4 below). PPPs can identify and measure threats for inclusion in NRAs and PPP activity may be instigated in response to risks identified in NRAs. The NRA can also contribute to further and ongoing risk identification and deepening of the risk understanding, which influences AML/CFT/CPF actions including supervision. Establishing and adjusting PPPs should reflect national priorities.

Figure 4. PPP – National Risk Assessment Feedback Loop



Source: Survey responses

Operational Information

54. Operational sharing delivers actionable intelligence that accelerates investigations and strengthens compliance and can comprise different categories, as listed below:

- Case-specific intelligence.
- Transactional information: Shared by jurisdictions typically through secure platforms such as Egmont Secure Web, THEMIS (e.g. Gibraltar FIU's secure platform) or bespoke platforms unique to each jurisdiction or PPP coordinating authority.
- Customer due diligence (CDD/KYC) data: Exchanged in controlled environments by countries, usually for case-specific investigations.
- Requirements of law enforcement agencies or judicial authorities.
- Financial metadata to support network analysis and tracing of illicit flows.

- Geo-location data: Provided in high-risk cases by some jurisdictions.
- Communications data: Shared by some jurisdictions, including Hong Kong, China, and Gibraltar, typically under court orders.
- Bulk data: Accessible in limited cases, subject to additional procedures and policies
- Biometric data: Considered special category data under GDPR and shared only under strict conditions.

55. Over half of jurisdictions participate in "deep" operational exchanges, which may include case-specific intelligence, transaction data, or customer due diligence (CDD) information (see case examples in Box 10 below).

Box 10. Operational information sharing PPPs bridging information gaps

Albania

In Albania, there are several PPPs for AML/CFT/CPF purposes. These typically involve collaboration between SPAK (Special Structure against Corruption and Organized Crime), the FIU Albania (DPPP), banks, DNFBPs, and other relevant private-sector stakeholders for different purposes.

Key PPPs in Albania include the "iPROCEEDS Project" established 30 January 2019 with a focus on combatting cybercrime and online crime proceeds. Operational work includes targeted joint meetings, intelligence sharing, and training. While initially single-issue-focused, the project has gradually integrated broader risks related to online financial crime and collaboration between public and private sectors.

Source: Albania

Malaysia

Malaysia developed Malaysia's Financial Intelligence Network (MyFINet) in 2017. There are six thematic working groups classed by crime type (Corruption, Smuggling, Securities Offences, Tax, TF and PF) under MyFINet. The main purpose of MyFINet is to facilitate a more systematic intelligence sharing on specific crime cases and topical issues between the FIU, LEAs and FIs. Between 2019 and February 2025, 61 cases were presented in the working groups meeting of MyFINet, and 44 disclosures by the FIU of financial intelligence information including detection of unlicensed virtual asset activity (See Box 6.6 in Malaysia's 2025 Mutual Evaluation).

Source: Malaysia

Legal and regulatory considerations of information sharing

56. Jurisdictions cited three primary reasons why information sharing is sometimes restricted:

- **Legal barriers or absence of gateways** – lack of legal or statutory basis to share non-public/operational data with private sector entities outside of traditional law enforcement and FIU channels;
- **Institutional limitations** – limited resources, lack of IT and technical infrastructure, fragmented public authorities resulting in misalignment of roles and expectations; and
- **Trust and cultural constraints** – concerns by both public and private sector stakeholders regarding information misuse or compromise, conservative mindset by public authorities regarding sharing of non-public/operational data.

57. Many respondents noted the importance of ongoing engagement with Data Protection Authorities (DPAs) for the development of a strong, adequate legal framework that breaks barriers (See Box 11 below) while many others have not yet engaged with DPAs. In terms of overcoming trust issues, survey responses highlight the role of starting with strategic information sharing before moving to deeper engagement.

58. Where lack of IT and technical infrastructure and resources are issues and in general for the setting up of first PPPs, some jurisdictions have approached technical assistance providers.

Box 11. Engaging with Data Protection Authorities for successful PPPs

Botswana

The FIU, in the context of its PPP (Botswana Public Private Partnership Task Force and Forum), cooperates with the data protection authority, the Data Protection Commission, ensuring it complies with its data protection legislation, and also collaborates in awareness programmes where the Data Protection Commission presents and raises awareness on the provisions of the Data Protection Act.

Source: Botswana

Information flows in Public-Private Partnership information sharing

59. There are three key parts in PPP information sharing 1) public-to-private, 2) private-to-public and (3) private-to-private. The first two are covered in other sections of this report when describing types of PPPs. On private-to-private mechanisms, these are sometimes enabled by, or exist within the framework of a PPP. Private-to-private information sharing is, in most jurisdictions, the least matured in the operation of PPPs and may require an enabling legal framework and enabling data infrastructure.

60. A case study and some examples of how some countries are developing in this field are presented in Box 12 below.

Private-to-Private Mechanisms

61. In the UK, two sets of legislation enable private-to-private information sharing:

- The Criminal Finances Act 2017 allows banks and other businesses in the regulated sector to share information with each other on a voluntary basis in relation to a suspicion that a person is engaged in money laundering, suspicion that a person is involved in the

commission of a terrorist financing offence, or in relation to the identification of terrorist property or its movement or use. The information sharing can be instigated either by a regulated sector entity or the UK National Crime Agency (NCA). Any member of the regulated sector is entitled to refuse to undertake such sharing. Where information is shared in good faith, there is no 'tipping off' offence. Any money laundering or terrorist financing reporting obligations that arise in the course of information sharing must be reported to the UKFIU (the UK's country FIU) in the usual way, i.e. a Suspicious Activity Report (SAR). However, this legislative provision is rarely used with only six instances of its use between 2020 and 2021 and nothing since.

- Separately the Economic Crime and Corporate Transparency Act 2023 (ECCTA) creates voluntary information sharing provisions that enable direct private-to-private UK based information sharing between businesses in the regulated sector for the purpose of preventing, detecting or investigating economic crime. UKFIU's working groups are actively improving private-to-private information sharing between its members, and upcoming cross-sector working group meetings facilitated by UKFIU have a specific focus on building relationships to encourage cross-sector private-to-private information sharing. Findings from across the UK financial sector demonstrate the tangible value of ECCTA information sharing in managing economic crime risk. In a sample of six financial institutions, 65% of investigations triggered by shared intelligence resulted in positive risk management action by the receiving institution.

Box 12. Private-to-private information sharing case study and mechanisms

UK Private-to-Private Sharing Case Study

Bank A shared information with Bank B under Section 188 of the UK Economic Crime and Corporate Transparency Act (ECCTA), warning of suspected money laundering activity. The warning related to a customer who had made a series of high-value cash deposits over a short period and rapidly transferred the funds to an account held at Bank B.

Using this information in conjunction with internal data, Bank B identified the customer was part of a large, interconnected network of individuals and businesses. The network was assessed as providing underground banking services.

The investigation identified that more than £10 million had moved through the network, comprising a mix of legitimate and illicit funds. As a result, Bank B submitted SARs and restricted more than £1 million across accounts linked to the network. Law enforcement agency subsequently secured £159,000 through Account Freezing Orders, and live criminal investigations remain ongoing.

The intelligence sharing enabled Bank B to take wider disruptive action. Bank B issued a further seven ECCTA information-sharing warnings to other financial institutions, supporting additional intervention across the financial system.

Bank B also developed their transaction monitoring rules, to detect similar activity. During testing alone, the new rule generated more than 200 alerts, resulting in over 80 additional SARs, the securing of a further £515,000 through Account Freezing Orders, and five new ECCTA information-sharing opportunities with other institutions.

This case demonstrates how timely and targeted information sharing, when used against organised criminal networks, can have a powerful force-multiplying effect - enabling financial institutions and law enforcement to identify hidden networks, disrupt criminal activity, and protect the wider financial system.

Source: United Kingdom

Private-to-private mechanisms

The Canadian Model for Private-to-Private Information Sharing

Private-to-private information sharing for deterring money laundering, terrorist financing, and sanctions evasion (AML/CFT/SE) purposes in Canada has been developed with appropriate guardrails and oversight in place to maintain strong data protection and privacy safeguards, while also being flexible enough for those who choose to voluntarily participate.

In 2024, amendments to Canada AML/CFT and Proceeds of Crime Act (PCMLTFA) introduced the ability of regulated private sector entities to voluntarily share

information with each other for AML/CFT/SE purposes. Regulations to operationalise these legislative changes came into force on 4 March 4, 2025, setting out the parameters for regulated entities to use the framework, including the obligation to develop and abide by an approved code of practice governing the exchange of information.

By sharing information, regulated entities will have additional information and data to support their ability to detect suspicious transactions, accurately assess risks, inform risk-based measures and support compliance with their obligations, including reporting suspicious transaction reports to FINTRAC.

Privacy protections for personal information are maintained by requiring codes of practice that are reviewed and approved by Canada's federal privacy authority – the Office of the Privacy Commissioner - to demonstrate that information sharing will comply with all relevant laws and maintain privacy protections that conform to Canada's federal privacy law. The Office of the Privacy Commissioner must formally approve a code of practice prior to any information sharing taking place, with a statutory review period of up to 135 calendar days for the Commissioner to decide.

Source: Canada

Germany SafeAML

In 2021, ML and financial fraud cost the EU an estimated EUR 133 billion. To prevent such activities, German and European regulations require banks to monitor financial transactions for suspected ML. However, due to data protection regulations, they are not permitted to exchange transaction data directly, which makes it difficult to detect criminal activities. Information requests allow for a limited exchange of information between financial institutions, but the current manual process is costly and time-consuming.

The SafeAML project supports financial institutions in combating ML by digitising existing communication processes for information exchange. This shall help reducing costs and detecting criminal activity more quickly. In addition, SafeAML enables the analysis of relationships between potentially suspicious transactions. The results of these cross-institutional analyses are shared only with the participating institutions. Neither EuroDaT nor third parties have access to the transaction data. The underlying procedure has been coordinated with the Hessian data protection authority.

The initiative has been "live" since the end of April 2025, which means that participants are now exchanging up-to-date information through the trustee.

Currently three German banks are connected to the network. The use of safeAML is open to all domestic and European credit institutions.

The initiative is facilitated by EuroDaT (which is owned by the state of Hesse) and aims to digitise requests for information. EuroDaT act as a 'trustee' of the information - all other participants requiring information must request it through the trustee who then matches the recipients with the data they require. Bafin is not directly involved in this initiative but is monitoring how it progresses, particularly with regard to the future European regulation of Article 75 of the AMLR. The initiative sees itself as a possible form of partnership within the meaning of that provision.

Source: Germany

Singapore's Collaborative Sharing of Money Laundering/Terrorism Financing (ML/TF) Information & Cases (COSMIC)

Singapore has a digital platform called the "Collaborative Sharing of Money Laundering/Terrorism Financing (ML/TF) Information & Cases", (COSMIC) which was co-developed by MAS and six major commercial banks. COSMIC currently focuses on three key risks identified by the national AML/CFT Steering Committee to be the priority targets for risk mitigation, namely 1) Misuse of legal persons, 2) Trade-base money laundering, and 3) Proliferation financing. COSMIC allows the participant banks to securely share with one another, information on customers whose accounts have been identified for potential financial crime concerns, which makes it easier for banks to detect and thereby deter criminal activities. MAS has access to all information shared on the platform to monitor if participant banks are using COSMIC appropriately, and support MAS' broader supervisory and surveillance role to ensure that financial institutions have robust defences against financial crime.

Source: Singapore

France's private-to-private platform to share information on accounts suspected to serve in fraud schemes

On 6 November 2025, the French Parliament has adopted a law on improving anti-fraud action in the banking sector, which provided a legal basis for private-to-private information sharing on fraud-suspicious accounts.

On this basis, the National Register of Accounts Flagged for Fraud Risk was launched on 7 May 2026. Hosted by the Banque de France, the French central bank, this new system enables banks and more broadly payment service providers to share reports on IBANs identified as suspicious, thereby strengthening the sector's collective ability to prevent wire transfer fraud. Once an IBAN is entered into the database, the entire banking community can be notified and adjust its pre-transfer verification procedures accordingly. This way private actors are able to mutually flag risks of fraud and to collectively improve fraud detection and prevention.

The system was designed with strict safeguards in place to protect personal data. No personally identifiable information is recorded in the database: only IBANs are reported. Furthermore, the recorded data is retained for a limited period (i.e. 13 months), commensurate with the requirements of the fight against fraud. These provisions aim to ensure a balance between the operational effectiveness of the system and respect for the rights of account holders.

Source: France

India's registry of mule accounts

National Cybercrime Reporting Portal (NCRP) – The Indian Cyber Crime Coordination Centre (I4C) has made available a negative registry of all mule accounts and KYC identifiers associated with such accounts on its portal. This registry can be accessed by all financial institutions as a risk indicator. The registry is being used as a risk indicator by financial institutions at the time of onboarding, as well as for ongoing due diligence and enhanced monitoring.

Source: India

Other relevant mechanisms from survey responses

The United States FinCEN's "section 314(b) mechanism" is a voluntary information sharing program between financial institutions under a "safe harbour" that offers protections from liability, in order to better identify and report activities that may involve ML/TF.

Within the UK's Data Fusion PPP, a Banking Sector Tactical Intelligence Group undertakes private-to-private information sharing. Mexico also has a mechanism supported by the Mexican Bank Association.

Domestic information sharing Public-Private Partnerships

62. This section is about the sharing of PPP information within a country. Approximately half of PPPs can share information outside of the core PPP participants albeit with some restrictions, such as limiting the type of data to strategic information, restricting the recipients to trusted entities or sectors (which may not include all reporting entities as trust is a precondition), anonymising the data, applying additional protections, safeguards and handling conditions restricting onward sharing or the data, or requiring legal authorisation or the written consent of information owners and/or PPP participants.

63. Information derived from PPPs may also be made publicly accessible when appropriate. For example, Latvia publishes strategic analysis reports derived from or connected to their PPP work in their FIU website, and Luxembourg shares sub-sectoral or vertical risk assessments. The UK's National Crime Agency uses its website i to publish JMLIT+ issued Alerts and a UKFIU magazine, which is also widely distributed every four months containing articles on trends, alerts and best practice guidance. UKFIU also publishes sanitised case studies that demonstrate

how SARs have supported investigations, and it makes extensive use of social media to distribute information to a wider audience.

64. As the coordinator of JMLIT+'s information sharing the UK's NCA is lawfully able to share information it receives from JMLIT+ participants with any other party it deems appropriate, provided it is for an NCA function and for a permitted purpose. However, it will always seek the consent of the core participant from whom the information originated. Canada publishes operational alerts and bulletins on its FIU website, providing typologies and indicators related to high-risk priorities through its PPP initiatives.

65. Canada's PPP model creates a direct channel for information to flow from the private sector to the public sector, enabling Canada's FIU to produce proactive financial intelligence on a range of high-risk crimes, including related to human trafficking, online child sexual exploitation, romance fraud, the trafficking of illicit fentanyl, illicit cannabis activity, and illegal wildlife trade. This model has allowed the FIU to contribute to proactive financial intelligence sharing to law enforcement based on information received from the private sector. It has increased the speed and the ability of the Canadian regime to proactively target more sophisticated crimes, across various PPPs.

Multi-jurisdictional and cross-border information sharing Public-Private Partnerships

66. Cross-border cooperation is widely recognised as essential to disrupt transnational ML/TF and predicate crime networks, with PPPs providing a structured avenue to enable such collaboration. Survey responses show consistent progress at the strategic level—particularly in the exchange of typologies, trends, and risk indicators—while operational cooperation remains uneven across jurisdictions.

67. Countries report improved understanding of financial crime typologies, enhanced risk assessments, and more effective investigations through coordinated actions such as joint evidence gathering and bilateral cooperation. Successful models demonstrate that translating strategic intelligence into operational impact requires clear legal gateways (e.g. MOUs with defined safeguards), secure and tiered information-sharing platforms, standardised typologies, and rapid-response channels for time-sensitive cases. Additionally, trust-building measures—such as joint training, secondments, and regular tactical engagement—play a critical role in enabling effective collaboration. Overall, while strategic information exchange is now well established, scaling operational cross-border PPPs will require continued legal, technical, and institutional development to transform these mechanisms into reliable tools for disrupting transnational crime.

68. Some PPPs include more than one jurisdiction by design (e.g. EFIPPP) considering common needs and interests while other domestic PPPs allow for information sharing cross-border with other countries that are not part of their PPP on an ad-hoc or case by case basis.

69. The EU's latest Anti-Money Laundering (AML) regulations package, specifically Article 75 of Regulation (EU) 2024/1624, presents significant opportunities to enable and facilitate the sharing and processing of information sharing between obliged entities and, where applicable, competent authorities through dedicated partnerships. To support this, EFIPPP has, under the leadership of the Chair of EFIPPP's Legal Gateways Working Group (LGWG) and in consultation with various partners, established a platform of experts. This platform aims to foster the exchange of ideas with the goal of drafting a practical guide for establishing a group under the legal framework of Article 75 AMLR.

70. Cross-border PPPs are most often FIU-led. Accordingly, they share information through the Egmont Group of FIUs and other information sharing platforms accessible to FIUs which represents an advantage.

71. Initiatives such as the Regional PPP being developed with support from the FATF-style Regional Body Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) also benefit from existing FIU-to-FIU work as noted in Box 13 below.

Box 13. ESAAMLG Regional Public-Private Partnership

ESAAMLG is currently initiating a Financial Information Sharing Public-Private partnership (FISP), established as a hybrid partnership combining strategic and operational elements, allowing for both typology development and case-based collaboration on high-risk financial crimes prevalent in the region. It aims to enhance the quality, relevance, and timeliness of suspicious transaction reporting; strengthen the analytical capabilities of FIUs; support proactive investigations; and ultimately contribute to the resilience and integrity of the region's financial systems.

Source: ESAAMLG

72. Several PPPs share information with international counterparts on a case-by-case basis, through different mechanisms (not just FIU-led exchanges), and in accordance with legal provisions, data policies and confidentiality safeguards. Other identified PPPs exchange information internationally more frequently, or indeed routinely, through both formal and informal arrangements. Notable examples include:

- **Singapore's Project FRONTIER+** highlights how different domestic PPPs can cooperate with each other on a transnational level. Initiated by Singapore's Anti-Scam Centre in October 2024, FRONTIER+ is a transnational alliance comprising anti-scam agencies across 13 jurisdictions (as of end-2025) to bring together scam-fighting strategies on a transnational level. Through this alliance, each anti-scam agency (which may itself be a domestic PPP) can cooperate with each other through the exchange of scam trends and best practices. Critically, this alliance also provides the foundation for real-time intelligence sharing, joint operations and coordinated enforcement against transnational scams and has resulted in positive outcomes. Two joint operations conducted by FRONTIER+ members in 2025 resulted in 2,100 subjects being arrested across all jurisdictions and the seizure of approximately S$28.2million from over 36 000 frozen bank accounts.
- **Australia's Fintel Alliance and Five Eyes** mechanism leads a public-private roundtable between FIUs from members of the Five Eyes mechanism[17]. FIUs share insights gained into current financial crime trends, increased understanding of new and emerging financial crime risks, and strengthening relationships regionally. International sharing is permitted by Australia's AML/CFT legislation.

[17] Australia, Canada, New Zealand, United Kingdom and the United States.

- **Gibraltar** actively participates in international sharing through its own PPP's membership of the EFIPPP, and its information exchange relationship with the UK's JMLIT+. Through these platforms, the PPP can share insights, typologies, and thematic intelligence, while also receiving valuable information from international partners, including JMLIT+'s Alerts, emerging typologies, red-flag indicators, and EFIPPP's research papers, which are then disseminated, where appropriate, to Gibraltar's PPP members to enhance their situational awareness and risk understanding. This reciprocal exchange strengthens both Gibraltar's domestic financial intelligence capability and its contribution to the broader international AML/CFT/CPF community, ensuring that Gibraltar's activities remain aligned with international standards and informed by the latest international developments and best practices. The FIU is also a member of the Quad Forum (a regional style strategic collective of FIUs). Through this it shares best practice via the PPP working group.
- **Quad Island Forum** - Whilst not a multi-jurisdictional PPP per se, the Quad Island Forum of Financial Intelligence Units of Gibraltar, Guernsey, Isle of Man and Jersey share learnings and best practices, and have collectively signed a Memorandum of Understanding (MoU) with the UK's National Crime Agency to facilitate exchanges of information between the Quad Islands' FIUs and the UK's JMLIT+ PPP. This is an interesting example of how a Regional PPP can be a step towards multijurisdictional ones.
- **United for Wildlife Financial Taskforce** – includes an information-sharing system, sharing the latest trends, red flags and typologies to help members identify and implement specific actions that the financial sector can take to combat wildlife trade. There are more than 60 financial institutions in the Taskforce, predominantly from banking (corporate, investment, online, retail and wholesale) and money service businesses. United for Wildlife has created 7 Regional Chapters to:
    - focus on regionally specific issues, allowing them to develop best practice and location-specific solutions
    - build trust across sectors with experts from LEAs, FIs, conservation and transport.

  The South African Chapter has collaborated with SAMLIT (South Africa's PPP) on financial investigations (and even re-opening old investigations) in high level illegal wildlife trade cases.
- **Canada's FIU (FINTRAC)** helped to launch Project Anton, an international public-private partnership that brings together domestic and international stakeholders to improve awareness of illegal wildlife trade and improving the detection of the laundering of proceeds of this crime. As part of this initiative, FINTRAC developed an Operational Alert using domestic strategic analysis, combined with international research and information contributed by Project Anton partners. The alert publishes indicators and typologies to help identify suspected illegal wildlife trade, supporting entities and authorities both within Canada and across jurisdictions in detecting related financial activity. Canada, led by the Canada Revenue Agency, also participates in the J5 – Joint Chiefs of Tax Enforcement and the Global Financial Institutions Partnership (GFIP), an international public-private partnership, committed to combatting transnational tax crime and ML. The GFIP includes representatives from tax authorities, FIs, and FIUs.

- **EFIPPP** - Within the European Union there is one transnational PPP – the Europol Financial Intelligence Public Private Partnership (EFIPPP), considered to be the first transnational information sharing mechanism ever established in the field of AML/CFT. Created in 2017, EFIPPP provides an environment for cross-border cooperation and information exchange between Europol, competent authorities (including FIUs and LEAs) and regulated financial service entities such as banks. Through its current 98 member institutions spanning over 31 EU and non-EU countries, including 17 LEAs, 28 FIUs and 30 FIs, as well as its observers (international organisations, banking associations and think-tanks) EFIPPP seeks to:
    - Build a common intelligence picture and understanding of financial crime risks
    - Facilitate the exchange of operational or tactical intelligence associated with ongoing investigations
    - Identify gateways for information sharing and support work on clarification of regulatory constraints
    - Promote the use of new tools for combatting financial crime
    - Support domestic and similar collaborative fora in relevant jurisdictions

  One of the recent landmarks was the publication of the "EFIPPP Practical Guide for Operational Cooperation between Investigative Authorities and Financial Institutions".[18]

- **Tunisia** established the Hannibal Platform in 2021 as an Application Programming Interface (API) and PPP to understand, identify and monitor the national risks of ML/TF related to the physical cross-border transportation of currency using blockchain technology connecting several databases including that of banks and exchange offices[19]. The Tunisian Financial Analysis Committee (CTAF), Tunisia's FIU can share information obtained through the Hannibal Platform with FIU counterparts. Below is a case study of how this platform helped detect a network of cash smugglers.

[18] Available at: https://www.europol.europa.eu/publications-events/publications/efippp-practical-guide-for-operational-cooperation-between-investigative-authorities-and-financial-institutions.

[19] FATF (2021), Opportunities and Challenges of New Technologies for AML/CFT, FATF, Paris, France, p. 33, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.inline.pdf (consulted 5 May 2026).

Box 14. Public Private Partnership and blockchain technology to detect cross-border cash smuggling

CTAF received a request for cooperation from Customs regarding an ongoing investigation on two Tunisian citizens that are importing significant amounts of foreign currency in cash from abroad to Tunisia and into the accounts of Tunisian companies. These companies allegedly engage in fictitious export operations and do not repatriate export proceeds, to fund their accounts and to evade legal prosecution. Investigations conducted by the Tunisian FIU using the Hannibal Platform and the passport numbers provided by Tunisian Customs, revealed the following: foreign currency import transactions carried out by the two suspects, including Customs Declaration Number, border office, declared amount, declaration date, and the amount settled for each transaction (the settled amount refers to the amount of currency imported from abroad that was exchanged or deposited into banking accounts); settled amounts; identification of not settled amounts; identification of the two companies that benefited from the deposit of the imported currency, their account numbers, the deposit date, and the branch where the transaction was executed; identification of the final destination of the funds deposited into the companies' accounts. Research identified that one of the suspects made two Customs Declarations using a recently issued passport that was not available to the Tunisian Customs authorities at the time of the request for cooperation. Other persons operating during the same period and who were not subject of the request for cooperation, were also identified as importing foreign currencies and then depositing the money into the banking accounts of the same Tunisian companies. Investigations using Hannibal Platform led to determine the total amount and the destination of foreign currencies imported by the two suspects, the identity of the beneficiaries, and to unveil the network of persons involved in the illegal cross-border transportation of physical currency.

Source: Tunisia.

73. The US has held several PPPs for specific purposes with Mexico and Canada. To clarify its legal basis, in 2025, FinCEN published a Cross-Border Information Sharing by Financial Institutions and SAR Confidentiality guidance document that clarifies that the Bank Secrecy Act does not prohibit cross-border sharing. The US Internal Revenue Service also participates in the J5[20] [21]Global Financial Institution Partnership and the J5 Cyber/Crypto Challenge.

74. Although there is no single international PPP, information can be shared from a domestic PPP to international sources. For example, information shared within the UK's JMLIT+ Groups must not be shared beyond the private sector participants, although it can be shared globally within each participant's own global group. The JMLIT+ Operations Group has shared selected operational information requests with other PPPs including the Australian Fintel Alliance, and has received and supported operational information requests from the US. The JMLIT+ is

[20] As noted previously, an intelligence alliance comprising Australia, Canada, New Zealand, the UK and the US.

[21] J5 refers to the Joint Chiefs of Global Tax Enforcement, a partnership of the Australian Taxation Office (ATO), the Canada Revenue Agency (CRA), the Dutch Fiscal Intelligence and Investigation Service (FIOD), the UK's His Majesty's Revenue and Customs (HMRC) and the Internal Revenue Service Criminal Investigation (IRS-CI).

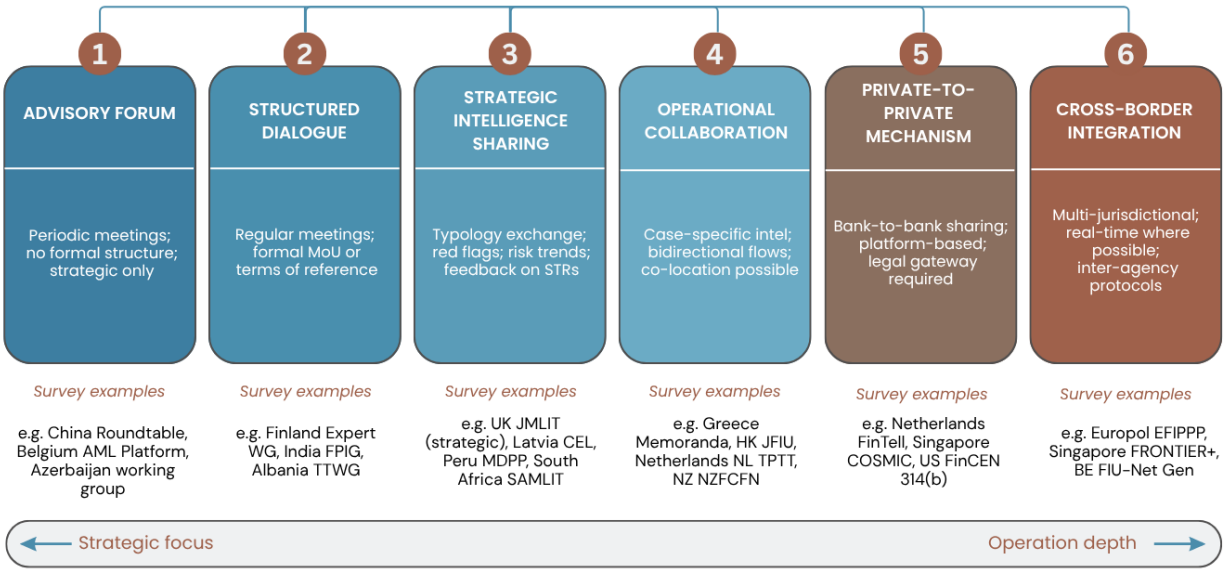
currently trialling the sharing of its operational and strategic information with partner PPPs in the UK's Crown Dependencies and Overseas Territories of Gibraltar, Guernsey, Isle of Man and Jersey. JMLIT+'s strategic Amber and Red Alerts are routinely shared with EFIPPP, UK Crown Dependencies and Overseas Territories, Five Eyes partners and international PPPs upon request.

75. Cross-border successes cited by survey respondents include enhanced communication and information sharing, joint investigations (including international asset tracing), strategic dialogue, capacity building and increased understanding of new and emerging financial crime risks through collaboration and knowledge transfer. Exchange visits for investigation and evidence collection also result as part of cross-border PPP collaboration and facilitate judicial cooperation. A greater global perspective of financial crime risk and mitigation helps optimise resources through combination of resources from both public and private sectors from different PPPs, to undertake more effective financial investigations and compliance efforts.

Evolution of Public-Private Partnerships

76. PPPs around the globe continue to evolve at their own pace, but are generally advancing, optimising, and improving collective capabilities in combatting AML/CFT. Nascent PPPs use strategic sharing as a trust-building mechanism, while mature PPPs are pushing the envelope and exploring more innovative ways to share and exploit sensitive data that supports specific cases. Some of this evolution is shown in the figures below.

Figure 5. Evolution possibilities for Public-Private Partnerships from advisory forums to deeper and cross-border integration

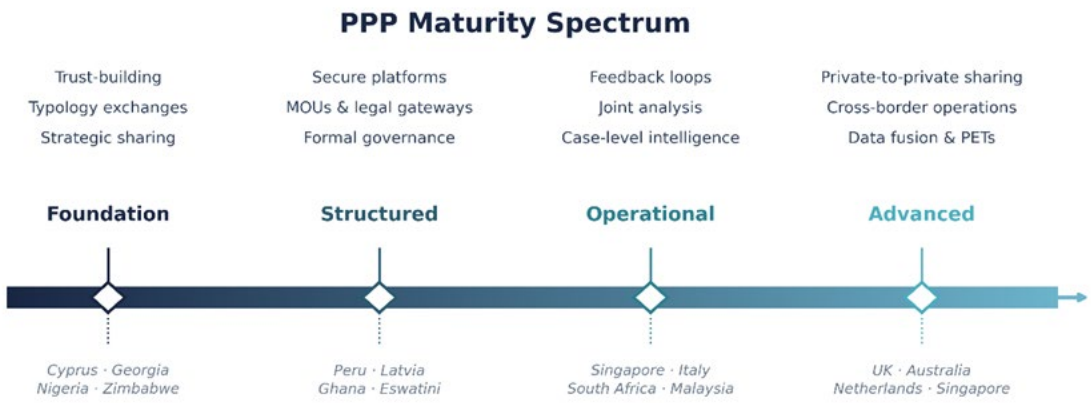


Note: Stages are not mutually exclusive. Some jurisdictions operate across multiple stages simultaneously. Examples are from Survey entries and are illustrative, not exhaustive.

Source: Survey responses.

77. PPPs in surveyed jurisdictions found themselves at different stages of maturity with trust and relationship building among the initial steps for some of them and progression to encouraging and/or facilitating information sharing on the other side.

Figure 6. Public Private Partnership Maturity Spectrum



Source: Survey responses

78. Early-stage PPPs in Cyprus, Georgia, Nigeria and Zimbabwe for example, are embarking on their journeys of PPP development.

79. The threat and nature of some specific threats (e.g. fraud) is driving innovative new PPPs, such as national anti-scam centres, which often rely on legal gateways facilitating seamless exchange of information between public and private sectors. More mature PPPs such as the Singapore Anti-Scam Centre continues to expand its strategic partnerships as scam threats grow in scale, speed and sophistication. For example, since its formation in 2020 with 30 stakeholders, Project FRONTIER has evolved to include more than 180 stakeholders (as of end-2025) as already noted above under cross-border PPPs, across both traditional and non-traditional AML sectors including financial institutions, FinTech companies, telecommunications firms and online marketplaces. This has shortened turnaround times for freezing bank accounts and enabled the recovery of more funds transferred to scammers. In 2025, Singapore's ASC recovered more than S$140million out of reported scam losses of more than S$900million.

80. The UK's JMLIT+ Data Fusion model is sharing datasets at scale, which are then analysed by its Joint Analytical Team (JAT), comprised of public and private sector data scientists, data engineers, intelligence officers and analysts, who identify targets, develop intelligence, disseminate intelligence packages to public and private sector partners, produce analytical products, and build tooling to automate processes and enhance data exploitation.

81. Evolution is also evident in the multi-jurisdictional space, with the Quad Island Forum, where the FIU's of Gibraltar, Guernsey, Isle of Man and Jersey who already work together and with the UK's JMLIT+ in the sharing of strategic information, but are embarking on a trial of operational information sharing.

82. For some PPPs, evolution means moving on to collaboration with non-bank partners such as the UK's JMLIT+ PPCF (Public Private Crypto Forum) within which the virtual asset sector proactively collaborates with UK law enforcement, regulators and partners from the wider industry to counter the criminal exploitation of virtual assets. See section 5.3.5 on membership.

83. For others, evolution takes the form of expanding scope or creating new PPPs to address emerging threat priorities. For example, the Department of Telecommunication in India has launched the Digital Intelligence Platform (DIP) to address fraud-related risks (see below).

Box 15. Evolutions in Public-Private Partnerships to address priority risks

The Department of Telecommunication in India has launched the Digital Intelligence Platform (DIP) which is accessible to reporting entities (banks and other financial institutions, etc.). The platform provides access to two risk indicators – Mobile Number Revocation List (MNRL) and Fraud Risk Indicator (FRI). The Mobile Number Revocation List (MNRL) is a list of mobile numbers which have been revoked by Department of Telecommunication based on investigations into complaints of fraudulent calls against such numbers. Similarly, the Fraud Risk Indicator is a risk indicator which assigns risk as 'low', 'medium' or 'high' to mobile numbers based on their linkage with internet banking transactions in respect of mule accounts which have been reported for cyber fraud, mobile numbers against which spamming complaints have been received, and other factors.

Source: India

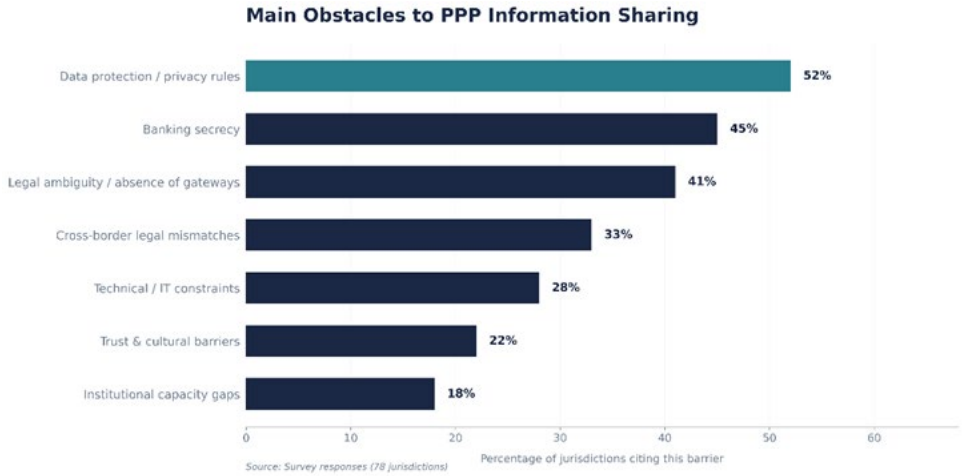
Canada established, among many PPPs, the Integrated Money Laundering Intelligence Partnership (IMLIP). The IMLIP aims to facilitate strong working relationships between large financial institutions and law enforcement agencies and support the permissible sharing of intelligence related to complex and sophisticated money laundering schemes.

Source: Canada

Secure, Privacy-Respecting Information Exchange

84. PPPs are sometimes restricted in the data they can share, due to data protection and privacy rules, banking secrecy laws, technical constraints, and other key considerations, as reflected below.

Figure 7. Main obstacles to information sharing



Source: Survey responses

85. Overall survey responses showed a wide variation in how PPPs operate and the challenges they face, not just in terms of data but other constraints, with some being more acute for lower capacity countries.

86. Survey responses reveal recurring themes such as legal constraints, operational limitations, technological shortfalls, cultural and trust deficits, data-governance and retention questions, and cross-border frictions; some of which are further described in the following section.

Legal and Regulatory Issues

87. Many jurisdictions reported that privacy laws, banking secrecy and statutory confidentiality sometimes restrict the flow of customer-level or case-specific information under a PPP. Around 41% of the respondent countries indicate that legal gateways influence the level of detail shared and mentioned strict data protection and banking-secrecy rules that require careful balancing of potential consequences of information sharing before any customer-level information exchange is made, and sometimes result in PPPs focusing on strategic rather than customer-specific information, at least at an initial stage.

88. PPPs involving personal data processing must comply with relevant data protection and privacy (DPP) requirements. Frameworks must ensure that data sharing complies with principles of necessity, proportionality, purpose limitation, and transparency.[22]

89. To support this, PPP initiatives should be supported by a Data Protection Impact Assessment (DPIA) to identify and document whether the personal data processed is necessary and proportionate to the purpose pursued. Data protection requirements can prevent discontinuation of business relationships and financial exclusion by imposing data controllers of PPPs to take into account the risk to individuals with a particular attention when operational data, special categories of data and sensitive data are processed.

[22] See also, United Nations Global Counter-Terrorism Coordination Compact, Ensuring Respect for Human Rights while taking measures to Counter the Financing of Terrorism, United Nations Global Counter-Terrorism Compact (November 2025), Section C - available at https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/hr_cft_guidance_november_2025.pdf

90. The strength and role of data protection authorities vary significantly across jurisdictions and directly affects how PPPs are designed and governed with positive developments as noted earlier in this report. In jurisdictions subject to comprehensive data protection frameworks such as the GDPR, formal consultation with DPAs is typically required before any information-sharing mechanism involving personal data is established. In the European Union, this is made explicit in Article 75 of the Anti-Money Laundering Regulation and requires supervisory authorities to verify, prior to the start of any partnership for information sharing, that appropriate compliance mechanisms are in place, in consultation with DPAs, and that a data protection impact assessment has been completed. In such frameworks, any information exchange involving personal data should be assessed for purpose limitation, proportionality, data minimisation, and legal basis.

91. Other jurisdictions, such as Singapore, maintain strong privacy governance through national legislation and engage DPAs in a structured way. In many jurisdictions, however, interaction between AML/CFT authorities and DPAs remains limited, which risks PPP frameworks that may lack adequate DPP safeguards. In some cases this was partly explained because the relevant jurisdictions did not report obstacles in information sharing and have very open or enabling legislation (e.g. broader access, powers circumscribed to AML/CFT purposes).

92. A central theme running through the document is the need to ensure that information sharing within PPPs operates in a manner compatible with DPP frameworks. Clear regulatory expectations and guidance are needed to avoid parties taking a "too cautious or conservative" interpretation of data protection laws to address part of this issue. Stakeholders may take a cautious approach, especially in cases where high level grounds may exist (e.g. legitimate interest), but these might not be supported by sufficiently detailed DPA guidance. Survey responses reveal that even where legal gateways exist, misinterpretation or a lack of clear guidance stands in the way of timely action.

93. This is why some jurisdictions have taken steps to clarify legal gateways and ensure confidence in sharing, which can also include using exceptions in legislation to share information in specific circumstances. Singapore established COSMIC under the Financial Services and Markets Act, offering clear statutory protection for information shared within the platform. Gibraltar developed formal Information Sharing Agreements (ISAs) similar to MOUs, coupled with extensive communication with industry, which helped institutions understand their legal position and encouraged participation. These examples suggest that legal barriers can be mitigated through clear legislative instruments in the case of operational information exchange or specific arrangements in the case of strategic information, combined with active stakeholder engagement and sufficiently detailed guidance.

94. Another significant finding concerns the limited use of Privacy Enhancing Technologies (PETs). Although a small number of jurisdictions experiment with pseudonymisation techniques or homomorphic encryption, the majority do not yet apply PETs in operational PPP contexts. Several reasons are cited: high cost, lack of technical capacity, limited vendor availability, regulatory uncertainty, and uncertainty about whether PETs can meet operational speed and accuracy requirements. In addition, it should be noted PETs are one tool within a broader DPP framework and do not substitute for the need for a clear legal basis, purpose limitation, and other applicable DPP obligations. Nevertheless, they have been useful for some countries, especially in a private-to-private context.

95. PETs, federated learning[23], secure multiparty computation (SMPC)[24], and homomorphic encryption[25], are increasingly used to facilitate collaboration without compromising confidentiality.

96. PETs advance secure and privacy-compliant private-to-private information sharing[26] and PPPs more broadly, particularly in the context of combating ML and TF. These tools provide innovative mechanisms for conducting joint analysis and intelligence generation without exposing sensitive or personally identifiable information (PII).

97. Some countries report the use of PETs or encryption within their PPPs as essential for securing sensitive information exchanges while others did not. Australia, Canada, the Netherlands, the United Kingdom and the United States stood out for incorporating secure analytical environments, encrypted communication channels, and pseudonymisation mechanisms to protect personal data during collaborative work between authorities and financial institutions. Mexico reported having a positive experience with the use of PETs (see Box.16 below).

[23] Federated learning uses a shared AI model to train across decentralised data sets.

[24] Secure Multi-Party Computation distributes a computation function to different datasets which are then recombined to reveal final outputs.

[25] Homomorphic Encryption enables analysis of encrypted data without having to first decrypt it.

[26] Consolidated FATF Standards on Information Sharing. See the FFIS Innovation and discussion paper: "Case studies of the use of privacy preserving analysis to tackle financial crime" (June 2020) - https://www.future-fis.com/the-pet-project.html

Box 16. Use of PETs by private-to-private information sharing

In Mexico, private-to-private information is facilitated by the use of a PET which operates as a decentralised interbank intelligence-sharing platform designed to enable financial institutions to exchange flagged clients and employee background information for the prevention of ML and financial crime more broadly, in real time and through an automated process. The platform's privacy-by-design architecture ensures that this exchange occurs without exposing the underlying personal data, addressing the confidentiality constraints that have historically limited information sharing between competing institutions. The platform operates on a fully decentralised infrastructure in which all data remains stored, processed, and encrypted within each institution's own security perimeter. A blind central node orchestrates the flow of information between participants but does not access, process, or retain any data at any point.

This is achieved through an architecture in which only the resultant hashes of clients' or employees' personally identifiable information travel through the central node, alongside catalogue values that institutions agree upon to characterise the nature of their suspicions. No names, account details, or raw data leave the originating institution at any point. An institution can either query whether a prospect has been flagged by another institution, or receive an alert if any of its clients are flagged by another institution — without either party's underlying data ever leaving its own security perimeter. The platform additionally supports direct institution-to-institution communication through an asymmetric encryption protocol in which only the parties involved in a given exchange hold the decryption key. The result is a technical architecture that structurally resolves the trust barrier that has prevented effective interbank cooperation in AML efforts — enabling institutions that operate in the same markets to collaborate on financial crime prevention without compromising data sovereignty or client confidentiality.

Source: Mexico

Confidentiality and integrity of criminal investigations

98. UN CTED assessments indicate that countries face challenges in institutionalising partnerships with the private sector on financial information-sharing and more specifically in the context of CFT, where a lot of information held by the public sector is classified and authorities are sometimes legally prevented from exchanging such information with private sector entities.

99. An effective, positive example is the Netherlands Terrorist Financing Task Force (NL-TFTF). The Netherlands started up the Terrorist Financing Public-Private Partnership Financial Expertise Centre (TF PPS FEC) Project, better known as the FEC TF Taskforce in 2017. The participants of the Taskforce are four public partners (the Netherlands Police, the Public Prosecution Office (the OM), the FIU-NL, and the Fiscal Intelligence Investigation Service (FIOD) and six private partners (ABN Amro, ING, Rabobank, ASN Bank, KNAB and Triodos Bank). This cooperation has been made permanent since 2019. The partners forming the taskforce share signals and the associated personal details of subjects related to terrorism. Such sharing of signals and reporting of unusual transactions takes place under strict legal

conditions. The provision of the subject related information is based on a provision in the Dutch Police Data law.

Operational and Institutional Challenges

100. PPPs face a broad range of operational issues. Mature PPPs, such as the ones in Australia and the UK, face challenges regarding scale and complexity. Australia and the UK's JMLIT+ and other jurisdictions' JMLIT+-type initiatives show potential scale-management issues from a participant's perspective: selecting appropriate operational partners from hundreds of licensed banks and payment providers, maintaining active participation, and avoiding unintended consequences such as de-risking by private participants.

101. Relatively recent PPPs will face different operational issues as they refine their process. For example, insufficient staff, limited technical expertise and fragmented inter-agency coordination. Ghana and Eswatini observe that some requests require validation by multiple agencies, which can extend processing times. The Marshall Islands and some smaller jurisdictions reported they are still at the early stages of PPP development and thus encounter basic governance and onboarding challenges rather than advanced integration issues.

102. There is also asymmetric maturity across sectors in many countries. The UAE and Indonesia reported scenarios where banks and large financial institutions are well-equipped to report under PPPs, whereas DNFBPs, VASPs and smaller firms may lack or have lower capacity. This asymmetry negatively affects the quality and consistency of intelligence uploaded and results in detection coverage gaps. Chinese Taipei's approach in creating an incentive for first-time or high-quality uploads is an example of one operational remedy to address these challenges through changing behaviours rather than merely through legal or technical solutions (See Box. 17 below).

Box 17. AML/CFT/CPF Information Exchange Platform Incentives to Boost Performance

To boost contributions, institutions and employees making first-time uploads or submitting high-quality content to the PPP are formally recognised. The supervisory authority and the reporting institution are notified by letter, which can be used as a basis for rewarding the contributing institution and its staff. The response also notes the need for a broader strategy and incentives across both public and private sectors.

Source: Chinese Taipei

103. Some jurisdictions have strengthened workflows by creating clear procedures and consistent engagement models. As mentioned above, the UK's JMLIT+ uses structured groups to manage information efficiently, and Hong Kong, China applies standard operating procedures supported by periodic briefings with participating institutions.

Technological and Infrastructure Limitations

104. Technological constraints can also be a barrier to effective communications and information exchange. Approximately 28% of jurisdictions mention system limitations, security requirements or platform differences as factors that influence the pace of information sharing. Australia notes that while secure platforms allow for the sharing of classified

information, access is also limited by members' ability to meet IT and security standards. Sweden has explained how differing data formats and the lack of common IT platforms limit the capacity to aggregate or analyse data. The Lao PDR mentioned limited IT infrastructure as one of the major challenges to establish effective PPP platforms while Myanmar and Nigeria are enhancing platforms for secure exchange. When agencies and private firms use different, sometimes incompatible formats and systems, interoperability problems arise, creating manual workarounds and increasing latency.

105. These limitations can result in reduced real-time information exchange, diminished analytical outputs, and an increased likelihood of elevated platform maintenance costs. In jurisdictions with more advanced technological capabilities, such as Singapore and Australia, the emphasis shifts from foundational access considerations to more sophisticated matters, including the scalability of data systems, the management of complex and extensive datasets, the facilitation of secure multi-party analytics, and the mitigation of risks associated with inadvertent disclosure. Growing appetite for big-data analytics and the resulting strain on infrastructure and governance models not designed for such scale is also discussed in the survey. However, the UK's JMLIT+ Data Fusion model has overcome some of these challenges, successfully sharing and analysing large scale datasets in a joint public/private resourced analytical team.

106. The use of privacy-enhancing technologies (PETs) varies across PPPs. There is little or no deployment of PETs in some PPPs, while others use it in a selective or experimental way. But even when used, there is recognition that PETs alone cannot solve legal or trust deficits; they have to operate within clear governance frameworks and be technically aligned with participants' capabilities.

107. Separately, several countries invest in secure technical platforms that support PPPs. Australia uses a tiered-access model that allows broad participation while maintaining appropriate security levels. South Africa has upgraded systems to improve connectivity between regulators and reporting entities, encouraging more structured information flows.

Cultural and Trust-Related Challenges

108. Sometimes PPP barriers are rooted in a simple lack of trust and commitment. In countries where PPP involvement remains voluntary and unrewarded, engagement is often sporadic and of variable quality. Banks and other private actors may be concerned about regulatory or reputational consequences for sharing sensitive information, especially if there is any legal uncertainty. Pre-launch concerns voiced about FLINT on behalf of Gibraltar demonstrate how building trust can be achieved through early engagement, open governance, and transparent information sharing agreements (ISAs). Lacking such measures, private actors hold back from sharing for fear of exposure or liability.

109. Trust is also built through reciprocity and feedback. In jurisdictions receiving little or delayed feedback, there is a weakening of private sector incentives to share. Formal structures, such as clear ownership, regular briefings, and clarity of legal position, ensure trust is institutionalised across large and complex PPP networks, as seen in the UK and Australia. Nigeria also strengthened assurance measures through designated contact points and clearer communication.

110. Deep cooperation goes beyond information sharing; it involves building a common language and genuine partnership between the public and private sectors.

Ensuring respect for fundamental rights (fair trial and presumption of innocence, privacy) and preventing unintended consequences (e.g. discontinuation of business relationships and financial exclusion)

Due process and fundamental rights

111. PPPs should be designed and should operate in a manner which respects fundamental principles of domestic law, and, when applicable, the principle of due process, including the right to a fair trial and the presumption of innocence. Appropriate mechanisms to assess the reliability and accuracy of PPP-derived data used in judicial or administrative proceedings are also important.

112. It should be noted that PPPs are not intended to circumvent procedural safeguards, including evidentiary thresholds to obtain judicial authorisation for coercive measures. Important factors to be considered in assessing compliance with these principles include:

1) the type of PPP (i.e. strategic, operational, hybrid), nature of activities undertaken, and the authorities involved (LEAs, and/or prosecutorial or judicial authorities);

2) the scope and conditions applicable to data requests, including relevant thresholds, the type of information to be exchanged, fundamental rights, including as regards the use of PPP-derived information in criminal proceedings; and compliance with applicable data protection requirements, including a clear legal basis, purpose limitation, and proportionality of the personal data processed.

113. A robust regulatory framework must ensure that any data exchange within a PPP adheres strictly to the principles of necessity, proportionality, purpose limitation, and transparency (see the section on legal and regulatory issues). These principles serve as an ethical and legal compass for balancing operational effectiveness with respect to individual rights.

114. In 2025, the United Nations Global Counter-Terrorism Coordination Compact released a Guidance on Ensuring Respect for Human Rights while Taking Measures to Counter the Financing of Terrorism, which offers specific recommendations on, inter alia, the use of relevant financial information obtained from the private sector, information sharing, and the establishment of partnerships with the private sector. The Guidance underscores principles applicable beyond TF PPPs, that PPPs should be designed and implemented in full compliance with international human rights law, including the principles of legality, necessity, proportionality and non-discrimination, and supported by robust safeguards on data protection, purpose limitation, retention, access and oversight. It further emphasises the need for clear governance, accountability and remedies to prevent undue de-risking, financial exclusion or adverse impacts on legitimate humanitarian and civil society activities.[27]

115. PPP design should be mindful that as a consequence of de-risking and denial of services, suspected individuals and networks may shift to less accessible platforms, leading to missed opportunities to collect information on illicit activities.

[27] https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/hr-cft_guidance_november_2025.pdf (section J).

116. The private sector, bound by data protection laws, is also required to respect human rights.[28] Without proper safeguards, public-private information-sharing can lead to bias and racial, political or religious profiling as clearly noted by UN CTED's Analytical brief which principles apply regardless of the threat the PPP may have been designed to address.

117. PPPs need to carefully assess the balance between effective information-sharing and safeguards against potential harm and consider integrating explicitly regulatory clarity and concrete guidance to the private sector on de-risking practices.

118. PPPs should also present opportunities to promote the meaningful involvement of civil society in ensuring that such partnerships do not infringe upon financial inclusion and civic space, including with respect to a chilling effect on legitimate operations of non-profit organizations and on exclusively humanitarian activities.

119. Last but not least, PPPs need to ensure that the typologies and preventive measures developed or tactical information shared within the framework of the PPP do not disproportionately affect any gender, including by limiting financial access.

Data Governance, Retention and Deletion

120. In line with the mutually supportive nature of DPP and AML/CFT objectives, PPP frameworks should ensure that data shared within them is governed by clear policies and procedures as required by applicable law, which may include purpose limitation, retention periods, access controls, and deletion procedures, consistent with applicable national law and relevant DPP standards. Several jurisdictions have confirmed that data shared under PPPs is subject to defined retention periods and deleted when the purpose for which it was collected expires.

121. Several jurisdictions have confirmed having a Personal Data Deletion requirement. Where this is the case, the obligation to delete data primarily arises in the following circumstances:

- when the purpose for which the data was collected and processed has expired;
- upon conclusion of an investigation where the individual is found not to be the perpetrator of the criminal act;
- when the original purpose for retaining the data has expired; and/or
- when a PPP participant withdraws from the Memorandum of Understanding (MoU).

122. Jurisdictions should ensure that deletion obligations, where required, are documented within PPP governance frameworks. Where national law grants individuals' rights over their personal data, PPP frameworks should set out clearly how those rights - in particular the right to erasure and the right to access - interact with AML/CFT retention requirements, and identify how the PPP should handle such requests. In addition, jurisdictions have also highlighted the lack of dedicated guidance on this interaction as a known source of friction.

123. The varied picture across jurisdictions points to the need for a common baseline: defined retention windows tied to processing purposes, audit trails, role-based access controls, and documented deletion procedures, applied consistently across all PPP participants. Several

[28] Guiding Principles on Business and Human Rights, Implementing the United Nations "Protect, Respect and Remedy" framework, 2011, available at: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf)

jurisdictions illustrate what good practice could look like in this area. Australia, South Africa and the UK apply clear retention schedules and deletion procedures. South Africa and the UK maintain defined audit trails and access controls, which create clarity for partners. Australia publishes guidance on data handling under its privacy legislation, supporting transparency and predictable governance. Georgia and Moldova are strengthening their frameworks, which supports clearer expectations for reporting entities. Nonetheless, some jurisdictions still lack defined or consistent practices which raises concerns about privacy compliance and auditability. Jurisdictions are encouraged to formalise these elements within their PPP governance frameworks and, to the maximum extent possible, engage their national DPP authorities in the design of PPP data governance arrangements.

De-risking and Unintended Consequences

124. Information from PPPs may influence how institutions approach higher-risk sectors, with de-risking being a potentially damaging side-effect of information sharing. JMLIT+-type partnerships reported examples where, upon receiving an alert or intelligence, private participants took the option of relationship termination rather than that of joint risk mitigation. For COSMIC, Singapore noted concern for possible risk transfer to non-participant banks and other jurisdictions highlighted phases where private partners de-risked entities flagged through PPP mechanisms. These patterns reveal that unless PPP outputs include guidance on proportionate risk management and regulatory expectations, private actors may choose the option of exiting relationships, which can drive illicit activity into less regulated channels.

125. Singapore provides clear guidance on proportionate risk mitigation and has set up a de-risking workgroup to discuss de-risking issues and practices to manage higher-risk customers without unnecessary exits. The UK follows up with industry on how to apply balanced approaches to account reviews, supporting consistent interpretations. Nigeria and The Gambia indicated that they continue supervisory dialogue to ensure institutions manage risk in a balanced manner. South Africa encourages banking institutions to consult with public sector investigation authorities prior to actioning matters dealt with in the PPPs. This practice has assisted with maintaining levels of trust which is critical to the operations of the PPP.

Issues relevant to cross-border Public-Private Partnerships

Legal and regulatory issues

126. Cross-border PPPs experience similar challenges to those experienced at a domestic information level but to a greater scale and complexity at times. The EU highlights the need for GDPR-compliant gateways especially in the context of Art. 75 developments where a greater number of PPPs within European jurisdictions is expected. Operational frictions and timeliness are particularly highlighted for cross-border information sharing. Where PPPs are not embedded within formal multilateral fora or MOUs, requests may be routed through traditional FIU channels (Egmont), sometimes adding layers of formality and time. Successful cross-border PPPs combine predefined contact points, escalation routes and time-bound replies to expectations; the survey responses show that where such mechanisms exist (for example, within EFIPPP or established JMLIT+ linkages) turnaround times and operational outcomes are demonstrably better.

127. On data protection, retention, deletion, and admissibility, influencing the types of information exchanged, cross-border exchange must satisfy both source and recipient data protection regimes. Survey replies show divergent practices on retention periods for PPP-shared data; some jurisdictions operate strict deletion windows and audit logs, while others have more ambiguous policies. These differences complicate sharing because a recipient

jurisdiction may be unable to meet the source state's retention/deletion commitments, or police may worry that evidence collected will not satisfy admissibility or chain-of-custody requirements in another jurisdiction. The absence of a clear legal basis for cross-border data transfers can pose a major obstacle and should be a major consideration for cross-border PPPs. The United States and some European respondents emphasised that legal constraints around evidence handling, and disclosure materially limit what can be transferred without court orders or mutual legal assistance. The practical lesson from the survey is that accepted templates for retention, purpose limitation, role-based access, and auditable destruction help bridge cross-border legal gaps when embedded in MOUs or ISAs.

128. The use of privacy enhancing technologies with regards to cross-border PPPs is still developing. Jurisdictions suggest four constraints to PET adoption across borders, necessitating careful consideration in their application: (1) differing legal views on whether de-identified data may still constitute personal data; (2) concerns around the technical maturity and interoperability of implemented PETs; (3) analytical limitations; and (4) cost and resource barriers for smaller partners. Where PETs are used in cross-border pilots, they support higher-risk sharing by allowing joint analytics on masked datasets; however, PETs do not remove the need for legal gateways or trust frameworks.

Technical issues

129. Technical capability influences how effectively jurisdictions share information. Australia notes that strong domestic systems do not always translate easily to cross-border PPP sharing because partners may have different encryption or classification standards, European jurisdictions use shared platforms (including SIENA) that facilitate alignment across borders.

130. Technical incompatibility shows up in two ways: platform and data standard mismatches, and security-classification differences. AUSTRAC notes that secure platforms enable richer exchanges but that partners vary in their ability to meet certification or encryption requirements. Australia's Fintel Alliance experience demonstrates that tiered security access is necessary; not all partners should need the highest clearance, but those differences require robust access-control logic and data-labelling standards. Sweden and Lao PDR reported legacy systems and limited IT capacity that force manual workarounds and increase the risk of data transcription errors. The absence of common message formats, taxonomy for typologies, and agreed metadata conventions makes automated cross-border analytics difficult. The responses show that jurisdictions with pre-agreed data schemas, shared taxonomies and interoperable platforms achieve faster, higher-quality cross-border analysis.

Trust, reciprocity and feedback loops

131. Trust and reciprocity are essential in cross-border PPPs just as they are in any domestic PPP. Countries that participate in established regional frameworks such as Gibraltar via JMLIT+ and EFIPPP benefit from built-in trust structures. Australia and Singapore maintain active communication with foreign partners to ensure transparency and shared understanding.

Derisking and unintended consequences

132. On potential de-risking and potential spillovers, cross-border PPPs sometimes produce unintended de-risking outcomes. The UK response reported cases where intelligence sharing caused some private institutions to exit relationships with flagged customers rather than engage in proportionate mitigation. Cross-border alerts can therefore displace illicit flows rather than disrupt them if receiving institutions adopt defensive withdrawal strategies. The survey evidence suggests a need for cross-border guidance on proportionate responses,

supervisory oversight that discourages blanket account closures, and mechanisms for joint risk mitigation plans across jurisdictions. Without these safeguards, PPP outputs risk amplifying the very vulnerabilities they intend to close.

Why These Challenges Persist and How Jurisdictions Differ?

133. The responses by many jurisdictions illustrate three structural reasons why the challenges of PPPs overall are sustained: First, legal systems pre-date the development of modern data-sharing needs, creating mismatches unless laws are updated. Second, technology change is rapid, with many institutions unable to match the pace of required upgrades. Third, trust and behavioural incentives are social problems to which technical or legal fixes can only partially solve.

134. Dominant constraints vary by jurisdiction. High-capacity states face challenges primarily around scale, governance and the avoidance of unintended harms such as de-risking. Middle-capacity states are concerned with legal clarity and the construction of secure platforms. Low-capacity states face basic challenges of staffing, technical resources and consistent policy. Where legal reform is possible and accompanied by practical governance (for example the UK, Singapore and Gibraltar), PPPs can achieve operational impact. In those jurisdictions where reforms are contested or opaque, PPPs are forced to operate in a limited, de-identified, strategic mode.

Achievements and Added Value of Public-Private Partnerships

135. Appropriate information-sharing allows all relevant stakeholders to make better use of available resources and innovative techniques to address financial crime. PPPs drive the private sector to enhance its capacity to mitigate high-risk activities and hence better support authorities in AML/CFT/CPF. This is essential considering the rapid evolution of financial technologies and the nature of such threats, which can involve low-value transactions that fall below monitoring or reporting thresholds, or be done in obfuscated ways. PPPs offer opportunities to combine the use of data and analytical tools and technologies with the shared public and private sector expertise on countering threats.

136. PPPs can be a way for private sector institutions, which are often unable to share essential information with each other, to warn the industry/sector about how money launderers and terrorist financers are exploiting products and services. PPPs can be instruments that provide opportunities for proactive sharing of relevant information, enabling the early identification of threats. They may also be mechanisms to address information exchange that requires immediate and urgent action.

137. Critically, operational PPPs are the most efficient method in many jurisdictions for overcoming the widely observed challenge of actionable information and intelligence being siloed within individual private sector or public sector organisations especially but not only on TF. With information exchanged on a real-time basis, multi-stakeholder PPPs allow for the design of more effective and comprehensive investigation strategies, as they enable public sector authorities to work with the private sector in tracking, mapping, and identifying terrorist networks more proactively.[29] Closer cooperation and coordination among different sectors are key, as they often cohabit the same processes and each holds a piece of the puzzle. For example, it is very common that a crowdfunding platform will have rich behaviour insights while the financial institution that powers their payments will have payment data. Understanding how to navigate this is crucial.

138. Private sector experts dealing with blockchain intelligence, innovative and AI-driven compliance tools, crowdfunding platforms and digital assets trade can offer their niche knowledge and leading technologies to assist authorities in detecting and suppressing terrorism financing, and to protect their sectors from TF abuse. For example, blockchain analytics companies provide transaction monitoring tools that offer the ability for compliant digital asset businesses to be protected from bad actors. This is critical because the private sector shares its knowledge on how these products and services operate, while the public sector identifies how they can be exploited for ML/TF purposes.

Evidence of increased ML/TF detection and criminal asset recovery outcomes

139. Jurisdictions that have implemented Public-Private Partnerships (PPPs) report significant benefits in strengthening AML/CFT prevention and detection measures. In the case of strategic information, such exchanges contribute to the early identification of emerging threats, risk indicators, and typologies.

---

29 https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/cted_analytical_brief_on_ppps_cft_2023.pdf. See also, materials of the launch expert discussions available at https://www.un.org/securitycouncil/ctc/news/cted-holds-multi-stakeholder-discussion-establishing-effective-public-private-partnerships

140. FIUs with more mature PPPs exchange STR-related indicators, CDD/KYC data, and financial metadata, thereby strengthening detection capabilities across the financial sector and DNFBPs. In addition, these partnerships facilitate structured feedback mechanisms, leading to enhancements in AML/CFT compliance frameworks within reporting entities. The primary benefits of operational information are reflected in the disruption of criminal networks, expediting investigative processes, and enabling access to more actionable intelligence. See for example, Box 2 on Indonesia's early detection of TF.

141. In spite of the benefits reported by some PPPs, establishing performance indicators and measuring the achievement of strategic objectives remains a challenge. It is critical to conduct both quantitative and qualitative monitoring and evaluation of PPP contributions, as this reinforces trust among stakeholders, promotes accountability, and ensures long-term sustainability. The example below from Austria provides an example of improved asset recovery results as a dedicated working group under its PPP.

Box 18. Improved asset recovery results as a result of a dedicated sub-group under the Financial Intelligence Network Austria (FINA)

Shell companies constitute one of Austria's most significant money laundering risks. FINA has prioritised this topic, most recently with the creation of a dedicated subgroup in early 2026. The cooperation of authorities and obliged entities has facilitated operational success:

- Before the sub-group, the financial police issued 117 freezing orders and issued confiscation orders for EUR 186 million in 2025.
- However, the results have almost doubled in just 6 months: By June 2026, it had already issued 181 freezing orders and had issued confiscation orders for EUR 18.2 million.

Source: Austria

Improvement of STR quality

142. The collaborative nature of PPPs enables the systematic sharing of typologies, indicators, and strategic analysis, improving the accuracy and justification of STRs by aligning them with emerging risks and national or even international priorities. Structured cooperation—through secure electronic exchanges and specialised forums—reduces information asymmetry between competent authorities and reporting entities, accelerating the submission of timely STRs with greater operational value.

143. Regulatory feedback and the publication of aggregated risk analysis promote consistency and standardisation, minimising duplication and improving traceability. Access to CDD/KYC data, sectoral risk trends, and risk-based guidance allows STRs to evolve from generic alerts to robust reports with analytical content that supports prioritisation and segmentation of investigations. Collectively, these practices—anchored in FATF standards and Egmont Group principles on secure information exchange—not only increase the utility of STRs for financial intelligence but also strengthen the system's capacity to detect complex patterns and mitigate systemic risks.

144. Data on the impact of PPPs on the quality of STRs is limited, as there is a lack of formal frameworks and metrics that can measure it. Yet the PPP as a discussion forum, the exchange of typologies, risk trends, red flags, and indicators, as well as access to strategic information and other elements (CDD/KYC data, financial metadata, STR indicators), have been found to contribute to reporting entities submitting STRs that are more comprehensive, relevant, and risk-aligned.

145. Countries such as Italy, Malaysia, Singapore, the UK and the US highlighted some of the positive developments they experienced: risk-based guidance, regulatory feedback, and specific data helps improve the structure, justification, and focus of STRs, shifting from basic reports to more precise submissions aligned with real patterns. See also Box 7 on Latvia's flexible and rapid approach which lead to targeted STRs and more effective outcomes.

Disruption of criminal networks

146. PPPs disrupt criminal networks by enhancing intelligence and information sharing, allowing proactive detection, faster investigations and better outcomes, and resource and expertise optimisation. Survey respondents highlighted how cooperation between public and private sectors translates into shared information that can be channelled into investigations of serious offences, providing a basis for action against networks and ML/TF schemes, and how PPP engagement improves joint understanding of patterns and supports authorities when they look for suspicious clusters across entities, providing a better base for network-focused investigations and improving the ability of authorities to understand patterns and act on them.

147. It is important to notice that the combination of operational data and risk indicators is considered useful to build a better and stronger foundation for investigations and follow-up against suspicious activity clusters. The statutory SARs regime and PPP information handling conditions support law enforcement use of SAR-based intelligence.

148. It is evident that PPPs are increasingly valued as an effective mechanism to mitigate criminal activities earlier, moving from a reactive and compliance-based model to a proactive and collaborative one, as they allow the pooling of resources, technology and specialised expertise that might not be available within a single public agency. See disruption case examples in Box 19 and 20 below. Box 12 on private-to-private information sharing supported by broader public-private partnership legislation is also relevant.

Box 19. Case Study: Fintel Alliance – Evolving Collaboration to Disrupt Cash-Based Money Laundering (CBML) in Australia

This Fintel Alliance case study encapsulates a number of PPP principles addressed in this report; demonstrating sustained partnership, trusted information-sharing, and privacy-preserving collaboration enabling a shift from reactive detection to proactive, system-wide disruption of CBML.

FIU-led strategic risk identification informed by NRAs and early public-private discussions within the PPP identified CBML typologies as high-risk ML channels that no single FI had complete sight of. In response, the PPP targeted operational projects, pooling industry expertise and financial data to improve understanding and test the emerging typologies.

Early collaborative work directly supported LE operations leading to convictions for proceeds of crime offences and the forfeiture of millions of dollars in illicit cash and assets, as well as firearms, drugs and encrypted devices. The activity also resulted in: a clearer understanding of CBML typologies including clustered deposits, cuckoo smurfing and exploitation of 3rd party account holders, a recognition of ML activity below reporting thresholds, and identification of vulnerabilities in existing financial system control measures, which were subsequently strengthened alongside the removal of high-risk cash deposit services.

Learnings were also translated into public financial crime guidance, and improved detection and reporting across the financial sector. Furthermore this activity was a catalyst for the establishment of the PPP's Collaborative Analytics Hub (CAH) as a proof-of-concept and from which subsequent CAH business-as-usual intensification activity brought FIU analysts, LE and industry secondees together to collect and analyse tens of millions of data points resulting in the identification of approximately AUD 4 million in suspected cuckoo smurfing activity, new persons of interest, investigative leads and enhanced internal bank reviews and reporting.

Source: Australia

Box 20. Example of a pyramid scheme dismantlement using a Public-Private Partnership (South Africa)

The South African PPP has an operational platform, namely the tactical operation group (TOG) which can address specified crime threats and specified subjects of interest.

In one case, a bank identified suspicious transactional activities on bank accounts of some of their clients. The analysis revealed the operation of a suspected pyramid scheme. It was suspected that the operators of the "work from home type" pyramid scheme were imitating a leading online store requesting members of the public to pay monies to earn commissions from sales.

A TOG was formed to expedite analysis on these suspicious transactions. It was discovered that three banking institutions had active bank accounts linked to participants in this financial scheme. Public authorities dealing with asset forfeiture and a financial regulator which regulates consumer protection and investigates unlawful pyramid schemes were requested to collaborate and join the TOG together with the banks. Through the TOG, the banks conducted expedited analysis of bank accounts and filed regulatory reports. This expeditious analysis process assisted the public authorities to obtain evidential information on the operation of the pyramid scheme. Multiple bank accounts of the eight most active participants in the scheme were analysed. The financial analysis revealed that multiple credit payments were received from members of the public. The account holders were transferring funds between their own bank accounts, including bank accounts of each other. Transactional references and patterns indicated cash deposits and credit receipts referenced with certain unique references. As a result of the TOG, the Financial Intelligence Centre issued directives to stop transactions in identified bank accounts, and the Asset Forfeiture Unit obtained a court order to freeze funds sixty (60) bank accounts to the value of about USD 458 000. Through the PPP, the banks and public authorities collaborated in an enhanced manner to identify and stop the operation of a serious financial crime.

Source: South Africa

Box 21. Public-Private Partnership collaboration resulting in the detection of multi-million trade financing scheme

Given Singapore's position as an international trade hub, Singapore is susceptible to the threat of trade-based ML. Through ACIP, an industry best practices paper was published in 2018 highlighting common trade-based ML red flags, typologies and best practices for identification and mitigation of trade-based ML risks. On an ongoing basis, ACIP monitors the trade-based ML risks and typologies, and banks regularly share their observations and measures adopted to mitigate risks.

These efforts have produced tangible and significant results. In 2019, an ACIP bank alerted CAD to Company A's under-invoicing, phantom shipments and suspected use of shell companies. CAD worked with banks to share information and intelligence through the ACIP case information sharing mechanism, and banks filed STRs relating to Company A. The Suspicious Transaction Reporting Office (Singapore's FIU) subsequently analysed the STRs and disseminated relevant information to CAD, allowing CAD to take swift and effective enforcement action. With the financial information and multiple reports lodged by banks and finance companies who had extended credit facilities to Company A for the purposes of trade financing, CAD commenced investigations into the former Chief Financial Officer of Company A in January 2020. She was convicted of 11 counts of cheating under Section 420 of the Penal Code 1871 (Penal Code) and one count of falsification of accounts under Section 477A of the Penal Code in January 2023. She was sentenced to imprisonment of 20 years for deceiving 16 FIs of more than USD 469 million.

Source: Singapore

Enhanced compliance capabilities of FI or DNFBPs

149. PPPs can significantly enhance AML/CFT/CPF compliance capabilities for FIs and DNFBPs by facilitating financial information sharing to prevent and detect illicit finance. These partnerships allow the public sector (including financial intelligence units and law enforcement) and the private sector (FIs, DNFBPs) to exchange information on new threats, criminal methods, and vulnerabilities more closely, including through anti-scam centres discussed. Scam response centres illustrate how FIs can share information on fraud typologies and suspicious activity, improving detection and response capabilities across payment flows.

150. Some countries note that the participation in PPPs helps institutions refine internal policies and monitoring practices, updating them in response to risk information, and strengthening overall AML/CFT compliance and highlight that existence of a legal framework, privacy impact assessments and structured channels with the private sector support improved awareness, stronger internal controls, governance and risk management in institutions.

151. Sharing strategic information and risk indicators across the financial system is considered key to improve risk-based approaches, establish adequate mitigating measures, better calibration of monitoring scenarios and alignment of institutional AML programs with national threat priorities. PPP platforms are used for providing risk guidance and feedback, which strengthens institutional risk assessment, thematic monitoring, governance and overall

AML/CFT compliance culture among banks, VASPs and DNFBPs and to integrate shared intelligence into their risk assessments, internal controls, monitoring models and compliance governance, strengthening AML/CFT capacity across banks, insurers, MSBs and other reporting entities. .

152. However, there is no mention of indicators to measure the improvement of compliance capabilities of FIs and DNFBPs, and this could be recommended as a measure of a PPP's impact.

Intelligence Sharing and Trust Building

153. Trust is the most frequently cited success factor in the global dataset. Effective PPPs cultivate it through structured engagement, balanced intelligence flows and constructive feedback.

- Strategic-first approach: Nearly all jurisdictions share strategic information—typologies (76.9%), red flags (75.6%), risk trends (76.9%)—making this the natural foundation for cooperation with fewer legal constraints.
- Controlled operational flows: Operational information sharing (case intelligence, CDD/KYC data, STR indicators) occurs in 55–65% of jurisdictions, but under clear legal basis and robust DPP safeguards. Secure systems and defined mandates significantly increase the willingness of the private sector to share.
- Robust feedback loops: Approximately 64% of jurisdictions provide STR/SAR feedback, improving reporting quality, reducing defensive filings and reinforcing shared risk understanding.
- Trust incubators: Regular meetings—strategic, operational or ad hoc—create a space for open dialogue on emerging threats and intelligence gaps, reducing uncertainty and informing future legal or technical reforms.

154. Effective PPPs combine structured processes with relationship-building, creating an ecosystem in which intelligence flows more freely and confidently.

Operational Structures, Technology and Resourcing

155. Operationally mature PPPs rely on secure technology, dedicated teams and multisectoral participation to support both strategic and operational workstreams.

- **Secure technological platforms:** Leading jurisdictions deploy encrypted, dedicated platforms such as COSMIC (Singapore), goAML-based secure exchanges, and the Fintel Alliance platform in Australia. These systems facilitate real-time information exchange with strong auditability and access control.
- **Multisectoral participation:** While banks remain the backbone of most PPPs, advanced models include DNFBPs, VASPs, professional service providers, telecom operators and digital platforms—sectors frequently targeted by cyber-enabled crime.
- **Dedicated resources and co-location:** Jurisdictions such as Singapore, the UK and Australia use co-location arrangements, where private sector analysts work alongside FIU and law-enforcement staff. This deepens trust and accelerates tactical decision-making by increasing the precision of the information sharing while ensuring each of the participants abide by the relevant confidentiality and data protection requirements.

- **Flexible exchange formats:** Best-practice PPPs combine quarterly strategic meetings, monthly operational working groups and real-time or ad hoc alerts when threats emerge.

156. These operational arrangements enable PPPs to scale, react quickly to threats and maintain analytical momentum.

Public-Private Partnerships as Bridges between Strategic and Operational Collaboration

157. Many PPPs are strategic, rather than operational. Strategic information—typologies, trends, red flags—is widely shareable, while operational information often faces legal, data protection and cultural constraints.

158. This "strategic-first, operational-when-possible" model is common globally and reflects:

- privacy and bank-secrecy rules,
- mandate limitations,
- institutional risk aversion,
- and the absence of explicit legal gateways for information sharing.

159. PPPs therefore function as bridging mechanisms, creating safe environments for dialogue, trust-building and early-warning exchanges that may later evolve into operationally capable structures as safeguards mature.

Conclusions

160. Among the broad variety of information sharing mechanisms PPPs stand out as permanent, effective instruments for combating ML/TF/PF when supported by a robust legal basis, clear governance, and technological innovation. PPPs have been implemented in all corners of the world.

161. Across the FATF Global Network, PPPs close critical intelligence gaps, enhance the speed and quality of financial investigations, and foster a culture of shared responsibility between governments and the private sector. PPPs especially allow interaction with sectors that may not be covered as reporting entities and therefore not captured by other information sharing mechanisms (e.g. social media and messaging platforms).

162. PPPs need to be established in a way that is not just compatible but collaborative with data protection authorities and related rules and principles. It is imperative to AML/CFT goals that data protection requirements do not unnecessarily impede legitimate efforts to fight financial crime that complies with relevant regulations. Countries need to establish common objectives and clear legal and regulatory expectations and carve outs, including through senior level engagement and joint guidance between the AML/CFT and DPP authorities. The FATF could explore how it can support this greater engagement between AML/CFT and DPP authorities.

163. Some jurisdictions continue to struggle with issues such as limited trust between stakeholders, strict data protection regimes, and insufficient technical capacity to sustain secure and efficient information-sharing channels.

164. These challenges underscore the need for a harmonised approach that promotes PPPs, combining legal clarity, institutional coordination, and advanced technology to achieve both operational effectiveness and compliance with international standards. The FATF can play a role in this regard.

165. The exponential rise of fraud around the globe also highlights the fragmented nature of domestic authorities and the need to cooperate more closely with FIs/VASPs, as well as non-traditional stakeholders. The threat can only be addressed by making appropriate information available to all relevant parties, and PPPs provide a high-speed road for information exchange.

166. Jurisdictions should be encouraged to adopt or strengthen PPP frameworks that are fully aligned with the FATF Recommendations and consistent with data protection principles. Pilot projects that integrate PET should be promoted to demonstrate how innovation can reconcile efficiency with privacy and legal compliance.

167. As a first step, PPPs can be structured through pilot initiatives or informal mechanisms (e.g. typology exchanges, discussion groups) to initiate a foundation of trust between the public and private sectors and to identify shared priorities, and assess any legal, regulatory, institutional barriers to cooperation. Over time, as the PPP matures, the relevant stakeholders should adopt an iterative process to progressively expand its membership, operational scope, and resource base, while developing a standardised and secure framework for collaboration. This process should support increasingly sophisticated forms of information sharing, including the exchange of non-public/operational data, in accordance with the applicable legal, regulatory and data protection requirements.

July 2026

www.fatf-gafi.org