EGMONT GROUP
OF FINANCIAL INTELLIGENCE UNITS

IEWG
INFORMATION EXCHANGE WORKING GROUP

EFFECTIVE PUBLIC-PRIVATE PARTNERSHIPS (PPPS)

Practical Guidance for Design, Governance and Operationalisation in the Fast-Changing ML/FT Context

Report

1. The Strategic Rationale for Public–Private Partnerships (PPPs)

Modern organized crime networks are structured to exploit institutional fragmentation. Criminals deliberately operate across multiple financial institutions, jurisdictions, and asset classes in order to ensure that no single entity sees the full picture.

Public authorities and private institutions each hold partial visibility:

- Public authorities[1] possess enforcement authority, classified intelligence, cross-sector oversight, and investigative powers.
- Private institutions[2] hold real-time transactional data, customer behavioural patterns, internal risk models, and operational detection systems.
- Together the public and the private sector holds the visibility of a countries reputation in regard to fighting ML/TF and predicate crimes effectively.

Therefore, a PPP becomes strategically necessary because:

- It reduces structural blind spots created by siloed data.
- It shifts the system from reactive reporting to coordinated prevention.
- It allows collective prioritisation of systemic risks instead of isolated institutional responses.

[1] Traditionally, public authorities with highest relevance for PPPs are: FIUs, law-enforcement authorities, prosecutors, supervisors, policymakers and ministries (in strategic and hybrid setup), tax and customs authorities, and security services. However, in specific jurisdictional cases, other public authorities could also be invited to participate. This is based on authorities' specific mandate, capacity and the PPP needs.

[2] Traditionally (but not mandatory in all cases), private sector is represented by financial institutions, VASPs, DNFBPs and NPOs – all being designated as reporting entities. However, other private actors (such as technology providers, academia, innovation hubs, social media and telecommunication providers, etc.) could also be invited, based on the specific needs of the PPP. Therefore, in essence, the private sector is represented by the most relevant parties in order to serve the specific needs of the partnership.

- It enhances the effectiveness of the risk-based approach by aligning supervisory signals with operational intelligence.

A PPP should therefore be understood as a systemic resilience mechanism, not merely an information-sharing exercise.

2. Preconditions for Establishing a PPP

Before launching a PPP, jurisdictions or regional/supranational bodies are encouraged to assess whether they have the institutional capacity, stakeholder commitment, operational maturity, and political stability needed to sustain the partnership over time. PPPs are long-term mechanisms that typically require phased implementation and continuous adaptation, which makes their sustainability vulnerable to political transitions, institutional reforms, regulatory changes, and shifts in national priorities. However, this assessment should happen before the PPP setup and therefore, it is not part of the current guidance.

2.1 Legal Feasibility

What information can be shared?

Clarity prevents both over-sharing (which may breach confidentiality, especially from the perspective of competent authorities) and under-sharing (which reduces effectiveness). Legal uncertainty and the lack of feasible and practical benefit from the PPP's participation are two of the main inhibitors of private sector participation.

Legal certainty can be achieved through a combination of complementary measures.

First, targeted legislative amendments may be necessary where current laws do not explicitly permit certain forms of information exchange. This is particularly relevant for strategic intelligence sharing, limited case-based exchanges under structured oversight, or private-to-private information sharing within an AML/CFT framework. Legislative clarification can define the categories of permissible information, establish proportionality principles, introduce safe harbour protections for good-faith participation, and clearly anchor PPP activity within the legal system. This approach provides the strongest and most durable form of certainty but may require political commitment and time.

Second, Memoranda of Understanding (MOUs) can provide procedural clarity. While they do not create new legal powers, they operationalise existing ones by defining scope, governance safeguards, confidentiality rules, access controls, and dispute resolution mechanisms. Well-drafted MOUs help ensure that all participants understand the boundaries and responsibilities of information exchange.

Third, safe harbour and liability protections are critical for private sector confidence. Institutions may hesitate to share information due to concerns about civil litigation, regulatory sanctions, or reputational risk. Explicit legal or regulatory confirmation that good-faith participation within approved PPP structures does not trigger liability reduces defensive compliance behaviour and encourages meaningful engagement.

Finally, operational standardisation reinforces legal certainty. Clearly defined templates, documented purpose limitation, structured access controls, and audit mechanisms ensure that information sharing remains controlled and proportionate. Even where the law is clear, poorly designed processes can create practical uncertainty.

In reality, legal certainty is rarely achieved through a single instrument. The most effective approach combines legislative clarity where necessary, authoritative guidance, structured governance arrangements, liability protection, and operational safeguards. Importantly, information sharing must not only be lawful, as it must be perceived by participants as legally safe and institutionally supported.

FIUs can play critical role in this process, not necessary by leading it, but by providing relevant practical information and clarity.

Under what conditions?

Define whether information exchange is limited to anonymized trends, aggregated indicators, or whether case-level exchanges are permitted. Conditions may include written requests, defined purpose limitation, or supervisory oversight.

Data protection constraints - PPPs must align with domestic data protection laws. Data minimisation principles should guide the design: only necessary data should be shared for clearly defined objectives.

In practice, data protection constraints affect PPPs in several concrete ways.

First, the principle of purpose limitation requires that personal data be processed only for a clearly defined and lawful purpose. In a PPP, this means that information shared must be directly linked to AML/CFT risk mitigation or crime prevention. For example, sharing a customer's full transaction history "just in case" would likely violate proportionality principles. However, sharing specific transaction patterns that indicate trade-based money laundering within a defined thematic working group may be justified if clearly tied to a documented risk objective.

Second, the principle of data minimisation requires that only the data strictly necessary for the defined purpose be exchanged. For instance, when discussing a typology involving shell companies, it may be sufficient to share anonymized behavioural indicators (e.g., rapid movement of funds through newly incorporated entities with no economic activity) rather

than identifiable personal details of account holders. Where case-based discussion is necessary, limited identifiers may be shared under controlled access rather than full datasets.

Third, lawful basis for processing must be clearly identified. Under data protection regimes such as GDPR, AML/CFT obligations often provide a legal obligation or public interest basis for processing. In practical terms, this means that the PPP's legal documentation should explicitly reference the statutory AML/CFT mandate as the lawful basis for data exchange. Without this clarity, institutions may hesitate to participate fully.

Fourth, storage limitation and retention rules must be respected. A PPP should define how long shared information may be retained. For example, if a working group reviews red flags related to sanctions evasion, documentation of the discussion may be retained for audit purposes, but identifiable personal data should not be stored indefinitely on shared platforms unless legally justified.

Fifth, access control is a critical safeguard. Not all PPP participants need access to all shared data. Role-based access restrictions ensure that sensitive information is visible only to authorised individuals directly involved in the relevant analysis. This reduces exposure risk and strengthens compliance.

Sixth, auditability and traceability are increasingly important. Secure platforms that log who accessed what information and when can demonstrate accountability. This is particularly useful if questions later arise regarding proportionality or lawful processing.

Seventh, anonymization and pseudonymization techniques can significantly reduce data protection risk. For example, during strategic discussions about suspicious activity trends, institutions can replace names with coded identifiers. If escalation becomes necessary, identifiable information can then be shared under stricter procedural safeguards.

Eighth, data subject rights must be considered. While AML/CFT frameworks often restrict certain rights (such as access requests that could undermine investigations), PPP structures must ensure that data protection obligations are not inadvertently bypassed. Clear documentation of legal exemptions and justification is important.

Finally, engagement with the Data Protection Authority can strengthen legitimacy. If a PPP model is discussed and informally aligned with the DPA in advance, participating institutions gain confidence that the structure is defensible.

However, in many instances (e.g. such as the Austrian and German PPPs, and EFIPPP) data protection was considered at a later stage, only one these partnerships matured to hold this kind of information. Therefore, PPPs might be also designed to be able to integrate this topic at a later stage.

In practical terms, respecting data protection law does not prevent effective PPPs. Rather, it requires structured design: clear purpose definition, proportional information exchange, limited access, secure storage, documented lawful basis, and audit mechanisms. When these safeguards are embedded from the outset, data protection becomes an enabler of trust rather than an obstacle to cooperation.

Safe harbour provisions - Private institutions must feel legally protected when sharing information in good faith. Without safe harbour protections, risk-averse compliance departments may limit meaningful engagement.

Strategic intelligence sharing legality - In some jurisdictions, legal frameworks allow operational case exchanges but are unclear on broader strategic trend sharing. This must be clarified to avoid institutional hesitation.

2.2 Strategic Alignment

A PPP must be anchored in documented risk priorities. Otherwise, discussions become hypothetical and non-inclusive. The partnership must be structurally and operationally linked to documented risk assessments and policy priorities.

The PPP should formally identify which documents constitute its strategic foundation. These may include National Risk Assessment (NRA); Sectoral risk assessments (banking, VASPs, DNFBPs, etc.); FIU strategic analysis reports; Supervisory risk outlooks; Law enforcement threat assessments; Sanctions risk analyses; International typology reports and mutual evaluation results (e.g. FATF). The key is not simply referencing them but extracting priority themes. For example, if the NRA identifies trade-based money laundering as a high vulnerability, the PPP should create a dedicated working group or structured workplan on that topic. This ensures alignment and legitimacy.

However, risk assessments are often high-level. A PPP must convert them into actionable themes.

The PPP should adopt a documented annual or biannual workplan that lists priority risks (e.g. sanctions evasion, professional money laundering networks, crypto-mixing services), assigns responsibility for leading each theme, defines expected outputs (e.g. typology paper, red flag update, guidance note), and sets timelines. Without a workplan, PPP discussions tend to follow the most recent headline event rather than strategic priorities. Nonetheless, not all risks deserve equal attention. In most instances, the PPP can use a simple matrix to identify its operational focus. However, this matrix should not be the sole way for decision-making, and it should always be added to the experts' opinion that eventually should have leading priority:

- High impact / high likelihood → Dedicated operational focus.
- High impact / emerging likelihood → Strategic monitoring group.

- Lower impact → Periodic review.

A risk-based approach improves inclusiveness because participation becomes relevance-driven. For example, if the focus is TBML, customs authorities and trade finance specialists should be invited. If the focus is crypto-assets, VASPs and blockchain analytics experts must be included. Risk anchoring naturally expands the PPP ecosystem in proportion to threat exposure.

2.3 Policy and Institutional Buy-In

Policy and institutional buy-in is a decisive success factor for any Public–Private Partnership. A PPP operates at the intersection of regulatory authority, market participants, and often sensitive intelligence. Without visible and sustained support from senior leadership, the initiative risks becoming symbolic, under-resourced, or risk averse. Buy-in matters for several reasons.

First, it provides legitimacy. When a PPP is endorsed at ministerial, supervisory board, or executive level, participation is perceived as part of the institutional mandate rather than an optional initiative. This reduces hesitation, especially where information sharing involves reputational or legal sensitivities.

Second, it enables decision-making authority. If institutions send representatives without sufficient internal standing, discussions may be constructive but ineffective. Senior endorsement ensures that representatives have the authority to commit their institutions to adjustments in internal controls, reporting practices, or resource allocation.

Third, buy-in protects the PPP during moments of tension. Sensitive discussions about compliance weaknesses, emerging threats, or supervisory expectations may generate institutional discomfort. Strong leadership backing allows the PPP to operate with strategic confidence rather than retreating into overly cautious behaviour.

Fourth, policy support ensures continuity. Financial crime priorities shift, leadership changes, and public attention fluctuate. Without institutional embedding, PPPs may fade over time. High-level endorsement anchors the PPP within the national AML/CFT architecture.

Achieving buy-in requires deliberate action.

One practical step is to clearly articulate the value proposition for decision-makers. Senior officials must understand how the PPP contributes to measurable outcomes such as improved STR quality, enhanced risk mitigation, better supervisory targeting, or stronger international reputation. Framing the PPP as a systemic risk management tool rather than a compliance forum increases executive interest.

Another key step is early involvement of leadership in the design phase. When executives are consulted before launch, rather than informed after structure is fixed, they are more likely to assume ownership. Presenting a structured concept note outlining objectives, governance, safeguards, and expected impact can facilitate endorsement.

Formalisation also strengthens buy-in. This may take the form of a ministerial mandate, supervisory board approval, or incorporation into national AML/CFT strategies. Embedding the PPP within official policy documents transforms it from an informal initiative into a recognised component of the financial integrity framework.

Resource allocation is central to genuine buy-in. A PPP requires dedicated personnel time, analytical capacity, secure communication infrastructure, and coordination support. Without clear budgeting, either financial or in-kind, participation becomes *ad hoc* and dependent on individual enthusiasm. Practically, this means that:

- institutions should designate dedicated liaison officers whose PPP responsibilities are formally recognised in their job descriptions.
- time commitments for meetings and working groups should be institutionalised rather than discretionary.
- technical infrastructure for secure communication should be funded and maintained.
- administrative support for coordination, documentation, and follow-up should be assigned.

Where possible, a small secretariat function, either within a public authority or jointly supported can significantly increase sustainability.

It is equally important to manage expectations realistically. A PPP cannot solve all ML/TF and predicate crime challenges. Setting achievable objectives and defining phased implementation (for example, starting with strategic risk exchange before moving to operational cooperation) makes leadership more comfortable supporting the initiative.

Transparency in reporting also reinforces buy-in. Periodic reports to senior leadership summarizing achievements, emerging risks, and measurable outputs demonstrate value and justify continued investment.

Finally, buy-in is strengthened when the PPP is positioned as enhancing existing institutional mandates. Public authorities retain investigative powers. Private institutions retain compliance autonomy. The PPP should be presented as a coordination mechanism that increases effectiveness without diluting accountability.

In summary, political and institutional buy-in provides legitimacy, authority, protection, continuity, and resources. It is achieved through early engagement of leadership, formal mandate, clear value articulation, structured governance, defined resource allocation, and

regular demonstration of impact. Without it, a PPP may exist on paper. With it, the partnership becomes an embedded and sustainable element of the national ML/TF and predicate crime response.

Rule of thumb: Senior management (with decision competences) on the governance level, subject matter experts on the working group level.

3. Governance Architecture of a PPP

3.1 Strategic Steering Layer

Defining overall objectives - Clear objectives prevent the PPP from becoming overly broad. For example, is the focus sanctions evasion, crypto-assets, trade-based ML, or fraud.

Defining overall objectives is one of the most sensitive and strategic phases in establishing a PPP. Objectives determine scope, resource allocation, and ultimately the credibility of the initiative. However, partners entering a PPP do not start from identical priorities.

Public authorities may prioritise disruption of high-impact criminal networks, strengthening of national risk assessment mitigation measures, or improving international ME outcomes. Supervisory bodies may focus on improving compliance quality and reducing systemic vulnerabilities. Law enforcement agencies may prioritise evidentiary value and prosecutorial success. Private institutions may prioritise regulatory clarity, risk mitigation, operational feasibility, and reputational protection.

If these differing priorities are not acknowledged explicitly, objective-setting risks becoming either overly broad or subtly dominated by one participant's agenda. To define overall objectives effectively, several practical steps are useful.

First, conduct a structured expectation-mapping exercise at the outset. Each partner should be invited to articulate:

- What problem they believe the PPP should address.
- What success would look like from their perspective.
- What constraints they operate under.
- What they are realistically able to contribute.

This exercise makes institutional incentives visible and reduces hidden misalignment. Of course, the alignment with the strategic rationale, as mentioned in section 2.2, should also be considered when determining the overall institutional incentives.

Second, distinguish between common objectives and partner-specific objectives. A common objective may be "reduce systemic exposure to sanctions evasion." A supervisory

authority may seek improved control frameworks. The FIU may seek earlier detection signals. Private institutions may seek clearer red flags and proportional expectations. These objectives can coexist, but they must be recognised as complementary rather than identical.

Third, ensure that objectives are framed in terms of risk reduction rather than institutional advantage. If objectives are perceived as serving primarily one stakeholder, such as enforcement statistics or supervisory pressure, other partners may disengage. Framing the PPP as a shared systemic integrity mechanism encourages balanced ownership.

Fourth, clarify roles in achieving each objective. For example, if the objective is to enhance detection of TBML:

- The FIU may provide strategic threat indicators and aggregated case insights.
- Supervisors may align inspection focus accordingly.
- Private institutions may adjust transaction monitoring scenarios and share detection challenges.
- Law enforcement may provide feedback on evidentiary usefulness.
- Explicit role allocation prevents duplication and avoids unrealistic expectations.

Fifth, ensure objectives are proportionate to each partner's mandate. Private institutions are not investigative bodies, and public authorities are not compliance operators. Objectives should respect institutional boundaries while encouraging cooperation within them.

Sixth, document the agreed objectives formally and review them periodically. Institutional priorities evolve due to political changes, emerging risks, or international developments. Regular review ensures continued alignment.

Finally, recognise that compromise is part of objective-setting. A PPP functions best when objectives reflect negotiated consensus rather than unilateral imposition. This negotiation process itself builds trust and shared ownership.

In practice, defining overall objectives is not merely about drafting strategic language. It is about aligning diverse institutional motivations into a coherent, balanced, and achievable framework. When partners see their priorities reflected in the objectives and understand their role in achieving them, they can fully commit and accountability increase significantly.

Reviewing performance indicators - Reviewing performance indicators is essential to ensure that a PPP remains credible, effective, and aligned with its objectives. Without structured performance review, a partnership risks becoming a discussion forum rather than a results-oriented mechanism.

Performance indicators serve several functions.

First, they provide accountability. A PPP typically involves resource allocation, institutional commitment, and reputational investment. Senior leadership in both public and private sector institutions, will expect evidence that the initiative delivers tangible value. Clearly defined indicators allow the steering level to assess whether objectives are being met.

Second, they reinforce strategic alignment. If the PPP was established to address specific documented risks, performance indicators should measure progress against those risks. This prevents mission drift and ensures that the partnership does not gradually shift toward less demanding but more comfortable topics. After all, the results from the work of a PPP should assist the jurisdictional or regional AML/CFT efforts, and not just present activities on paper, or only quick wins.

Third, regular reporting on measurable outputs and outcomes helps justify continued resource allocation and leadership support.

In practice, performance indicators in a PPP should be structured across different dimensions.

Operational indicators may include:

- Improvement in the quality and relevance of suspicious transaction reports in targeted thematic areas.
- Reduction in response time for urgent information exchanges.
- Increase in joint typology outputs or red flag updates adopted by institutions.
- Enhanced asset freezing or disruption actions linked to PPP-related intelligence.
- Increased consistency of detection practices across participating institutions.

Strategic indicators may include:

- Integration of PPP findings into National Risk Assessments.
- Updates to supervisory guidance reflecting PPP analysis.
- Evidence that thematic vulnerabilities are being mitigated.
- Inclusion of PPP outputs in international evaluation processes.

Engagement indicators are equally important, such as:

- Attendance rates, consistency of participation and leading/steering the work of specific PPP groups.
- Diversity of participating institutions.
- Feedback from members regarding usefulness and trust.
- Degree of follow-through on agreed action points.

Importantly, performance measurement should not focus solely on quantitative metrics. Financial crime prevention often involves qualitative improvements, such as better understanding of complex typologies or improved dialogue between institutions. Structured qualitative assessment through periodic surveys or structured reflection sessions, can capture these dimensions.

A practical approach is to require the strategic steering layer to conduct an annual performance review based on predefined indicators. This review should answer three core questions:

- Are we addressing the risks we committed to address?
- Are we producing measurable improvements?
- Are adjustments to structure, priorities, or resources required?

Performance review should not be punitive. Its purpose is adaptive governance. If indicators reveal limited impact, the response should be structural refinement rather than blame allocation.

In addition, PPPs may differ significantly in how their outputs are disseminated, and this is an important design choice that should be made early in the process. In some cases, PPPs operate as closed partnerships, where results - such as typologies, red flags, or operational insights, are shared only among participating members. This approach can facilitate more candid discussions and enable the exchange of sensitive or operationally relevant information, as participants may feel more confident that their contributions will remain within a trusted circle. Closed models are particularly suited to operational or tactical PPPs, where confidentiality, speed, and precision are critical.

In other instances, PPPs adopt a more open dissemination model, where selected outputs typically strategic insights, typologies, or general risk indicators, are shared more broadly with the wider financial sector or even published publicly. This approach enhances the preventive impact of the PPP by extending its reach beyond the immediate participants and supporting a more consistent understanding of risks across the system. Many mature PPPs apply a hybrid approach, combining both models, namely:

- Sensitive operational exchanges remain restricted
- Strategic outputs are disseminated more widely.

The choice between closed, open, or hybrid models should reflect the sensitivity of the information, the objectives of the partnership, and the desired balance between trust within the PPP and broader AML/CFT systemic impact.

Finally, transparency in performance reporting reinforces trust. When participants see concrete evidence of progress, commitment deepens. When challenges are openly acknowledged and addressed, institutional maturity increases. **In essence, reviewing**

performance indicators transforms the PPP from a static coordination mechanism into a dynamic, accountable, and strategically aligned instrument of ML/TF and predicate crime prevention.

3.2 Operational Working Groups

Analyse typologies – PPP typology analysis converts anecdotal case knowledge into structured detection frameworks.

Analysing typologies is one of the most substantive and value-generating functions of a PPP. It is the process through which fragmented case experiences are transformed into structured knowledge that can improve detection, supervision, and enforcement across the system.

A typology is not merely a description of a crime method. In a PPP context, it is a structured explanation of how a crime scheme operates, what indicators reveal its presence, where systemic vulnerabilities lie, and how institutions can respond proportionately.

The first practical step in analysing typologies is selecting the thematic focus. This should be anchored in documented risk priorities, such as TBML, sanctions evasion, misuse of legal persons, professional money laundering networks, or abuse of virtual assets. The selection must be justified by risk severity and systemic relevance. In some instances, some form of scoring should also be considered in order to allow prioritization when resources are not sufficient to cover the entire thematic priorities.

Once a theme is identified, the PPP should gather inputs from multiple perspectives.

The FIU may contribute aggregated case patterns and intelligence-derived behavioural signals. Supervisory authorities may provide findings from inspections that reveal control weaknesses. Law enforcement may highlight evidentiary gaps or investigative challenges. Private institutions may present anonymized case studies or monitoring challenges encountered in practice.

The objective is to build a multi-layered understanding of the scheme. For example, in analysing sanctions evasion typologies, the group might examine how corporate structures are layered across jurisdictions, how payment chains are structured to avoid detection, and where transaction monitoring scenarios fail to capture indirect exposure.

A key practical element is distinguishing between descriptive and analytical typology work. Simply describing past cases adds limited value. Analytical typology work should identify:

- Trigger events or behavioural anomalies.
- Common structuring techniques.
- Exploited regulatory or operational gaps.

- Indicators that can realistically be embedded in monitoring systems.
- Limitations in current detection approaches.

The output should be actionable. This may include refined red flags, updated transaction monitoring parameters, guidance notes for compliance teams, or recommendations for supervisory focus.

Another important aspect is ensuring proportionality. Typology analysis should not lead to unrealistic expectations or excessive defensive reporting. If red flags are overly broad or insufficiently contextualised, institutions may generate excessive false positives. Therefore, typologies must be tested for operational feasibility before dissemination.

Typology analysis should also be iterative. Financial crime methods evolve. A typology developed two years ago may no longer reflect current behaviour. Periodic reassessment ensures that knowledge remains relevant.

It is equally important to manage confidentiality during typology discussions. Case examples should be anonymized or structured in a way that avoids exposing identifiable individuals or institutions unless strictly necessary and legally permissible.

Finally, typology analysis strengthens trust within the PPP. When partners see that their contributions translate into improved collective understanding and practical guidance, participation becomes meaningful rather than symbolic.

In essence, analysing typologies transforms the PPP from a coordination platform into a knowledge-generation mechanism. It enables the partnership to anticipate risk, refine detection, and reduce systemic vulnerability in a structured and collaborative manner.

Identify red flags - Jointly validated red flags improve consistency across institutions and reduce false positives.

Identifying red flags within a PPP is not simply an exercise in compiling warning signs. It is a collaborative process of converting multi-source intelligence, supervisory findings, and operational experience into structured and implementable detection indicators.

Red flags serve as early warning signals. When properly designed, they help institutions identify suspicious behaviour before criminal schemes mature or dissipate assets. When poorly designed, they create excessive false positives, compliance fatigue, and defensive reporting.

The first step in identifying red flags is grounding them in typology analysis (as mentioned above). Red flags should emerge from structured examination of real cases, not abstract speculation. For example, if typology analysis reveals that TBML schemes often involve

repeated amendments to letters of credit shortly before shipment, that behaviour may become a red flag for enhanced scrutiny.

Second, red flags must be behavioural rather than purely formal. A red flag that merely describes a high-risk jurisdiction or a complex corporate structure is insufficient. Instead, the focus should be on patterns of activity. For example, rapid movement of funds across newly established entities with no visible economic footprint is more operationally meaningful than simply flagging offshore incorporation. A good example in that direction are the red flags created within the IEWG Laundromats project (link).

Third, red flags should distinguish between primary indicators and contextual indicators. A primary indicator may signal a direct risk pattern, while contextual indicators provide supporting evidence. This layered structure helps compliance teams apply proportionate responses rather than triggering automatic escalation for every isolated signal.

Fourth, red flags must be operationally feasible. During the PPP process, private institutions should assess whether proposed indicators can realistically be embedded into transaction monitoring systems (predictable models and patterns). If a red flag requires data that institutions do not collect, or requires subjective interpretation without objective criteria, it will not function effectively in practice.

Fifth, red flags should be tested against proportionality principles (in practice, as part of the PPP). Overly broad indicators may generate large volumes of alerts with limited intelligence value. A PPP should discuss how to calibrate thresholds so that detection is both effective and manageable.

Sixth, red flags should include explanatory context. Institutions are more likely to apply indicators effectively if they understand the rationale behind them. A red flag accompanied by a short explanation of the typology and risk mechanism enhances internal training and consistency.

Seventh, periodic review is essential. Same as with typologies, criminal methodologies evolve. A red flag related to early crypto-mixing services may become obsolete as new decentralised tools emerge. The PPP should establish a review cycle to update and retire outdated indicators.

Eighth, red flags should feed back into supervisory and FIU processes. If a PPP develops improved detection indicators, supervisors may adjust inspection focus accordingly, and FIUs may refine their analytical prioritisation.

Importantly, red flag development within a PPP is not about imposing prescriptive monitoring rules on private sector. Rather, it is about co-developing informed risk indicators that enhance collective detection capacity while respecting institutional autonomy. It is more about uniformed and shared understanding on the risk indicators development.

When properly structured, the identification of red flags becomes one of the most tangible outputs of a PPP. It translates strategic dialogue into operational enhancement and strengthens both prevention and disruption capabilities across the financial system.

Draft operational guidance - Written outputs ensure that PPP insights translate into internal control improvements. Operational intelligence sharing, especially when it involves targeted individuals or entities, significantly increases impact, but also legal and governance complexity.

Operational intelligence within a PPP refers to the structured sharing of targeted information about specific individuals, entities, networks, or transactional patterns that are assessed as presenting elevated ML/TF and predicate crimes risk. Unlike strategic typology discussions, operational intelligence is time-sensitive, potentially case-linked, and may directly influence monitoring or investigative action. This form of exchange can significantly enhance early detection and disruption. However, it must be handled with particular care.

When competent authorities share targeted individuals or entities, the purpose must be clearly defined. The objective is not to outsource investigation to private institutions, nor to create informal blacklists. Rather, it is to enable enhanced monitoring within legal and proportional boundaries.

For example, an FIU or law enforcement body may identify a network of legal entities suspected of facilitating sanctions evasion. Within a structured PPP setting, authorities may share:

- Identifiers (where legally permissible),
- Known associated entities,
- Behavioural patterns observed,
- Transactional characteristics linked to the activity,
- Geographic or sectoral exposure patterns.

The value for private institutions lies not only in the name itself, but in understanding the behavioural indicators surrounding the activity. This allows institutions to review exposure internally and assess whether similar patterns are present.

Several safeguards are essential.

First, legal basis must be explicit. Authorities must ensure that sharing identifiable information is grounded in statutory AML/CFT powers or other lawful bases. Ambiguous or informal sharing creates legal and reputational risk.

Second, purpose limitation must be clear. Information should be used strictly for risk assessment, monitoring, and compliance purposes. It should not automatically trigger account closure or adverse action without independent internal assessment.

Third, PPP frameworks must avoid creating *de facto* sanctions regimes outside judicial processes.

Fourth, access controls are critical. Targeted intelligence should only be accessible to authorised representatives within participating institutions, and redistribution should be prohibited without consent.

Fifth, documentation and auditability must be ensured. It should be clear when information was shared, under what authority, and for what purpose. This protects both public authorities and private institutions. Exchange of classified information should be avoided to the extent possible.

Operational intelligence exchange may take different forms.

- One approach is direct targeted sharing in urgent situations: for example, where asset dissipation risk exists. This requires predefined crisis protocols.
- Another approach is pattern-based operational sharing, where authorities describe characteristics of a specific network without disclosing full identifiers, allowing institutions to screen internally and revert if matches are found.
- A third model involves structured information requests, where authorities provide partial identifiers and request voluntary feedback within legal limits.

Operational intelligence within a PPP can dramatically increase disruption capacity. It allows private institutions to act as early detection nodes while respecting their legal boundaries.

However, this model should be introduced progressively. Many PPPs begin with strategic and typology-based cooperation before moving toward operational exchanges. Institutional maturity, legal clarity, and trust levels must be sufficient before implementing targeted intelligence sharing. Taking gradual steps increases the overall maturity and effectiveness of the PPP. That doesn't mean that this approach should be applied in all instances, but it provides better success chances and reduces potential leaks and other operational risks in front of the PPP.

When carefully governed, operational intelligence exchange transforms a PPP from a knowledge-sharing platform into a coordinated risk mitigation mechanism. When poorly governed, it risks legal challenge, reputational damage, and erosion of trust.

The balance lies in structured design, explicit legal grounding, proportional use, and strong safeguards.

3.3 Technical and Data Subgroup

Secure data exchange protocols - Secure data exchange is often reduced to "use encryption" or "use a certified platform," but that is only one layer. True security in a PPP is multidimensional: legal, technical, organisational, and behavioural.

Secure data exchange protocols in a PPP must combine technical safeguards with governance, operational discipline, and institutional accountability. Technology is essential, but it is not sufficient on its own.

First, technical infrastructure must be robust. This includes encrypted communication channels, certified secure platforms, role-based access control, multi-factor authentication, audit logs, and cybersecurity monitoring. Where appropriate, privacy-enhancing technologies (PETs) such as secure multi-party computation or federated learning may allow analytical collaboration without exposing raw data. This allows the exchange and analysis of fully encrypted data and enhanced the sharing capabilities of PPPs. Platform governance in terms of ownership of digital tools must be defined: who manages access and who audits digital activity.

However, secure exchange begins before data is transmitted. Clear classification of information is essential. PPP participants should define categories such as strategic information, anonymized operational patterns, and identifiable operational intelligence. Each category should have predefined handling rules. Without classification standards, participants may either overshare or apply inconsistent protection levels.

Second, strict access governance must be embedded institutionally. Only designated and authorised individuals should have access to PPP exchanges (e.g. Fintel Alliance). Participation should not depend on informal delegation. Institutions should formally appoint representatives and maintain internal logs of who can access PPP-related information. Role-based access ensures that sensitive intelligence does not circulate unnecessarily within organisations. This can happen within the PPP itself and could be based on the broader data protection rules in the jurisdiction. Therefore, in the majority of cases, no specific framework should be created for the PPP. Of course, this differs in the case of transnational PPPs, where (in absence of Supranational Legal Framework) a more formal international agreements should be established.

Third, purpose limitation must be operationalised. Secure exchange is not only about preventing external intrusion, but also about preventing internal misuse. Shared information should be used solely for the agreed AML/CFT purpose. Internal policies should clearly prohibit secondary use for commercial advantage, competitive intelligence, or unrelated compliance activities.

Fourth, clear third-party rules are essential. Information received through the PPP should not be further disseminated, both internally and externally, without explicit consent from the

originating authority (author). These rules must be documented and acknowledged by all participants. Trust is heavily dependent on respecting these boundaries.

Fifth, retention and deletion policies must be defined. Secure exchange includes secure disposal. PPP frameworks should specify how long shared information may be retained and when it must be securely deleted. Indefinite storage increases both legal exposure and cybersecurity risk. Deletion process could also be described.

Sixth, auditability and traceability should be built into the system. It should be possible to reconstruct who accessed what information and when. Audit trails provide accountability and deter misuse. They also protect institutions if later scrutiny arises.

Seventh, incident response protocols should be agreed in advance. In the event of a data breach, unauthorised disclosure, or suspected misuse, the PPP should have predefined escalation procedures. This includes notification obligations, mitigation measures, and communication protocols. Proactive preparation reduces damage in crisis situations.

Eighth, staff training and awareness are often overlooked but critical. Even the most secure platform can be undermined by poor operational behaviour, such as downloading sensitive files to unsecured devices or discussing confidential information outside authorised settings. Participants must receive regular training on secure handling obligations.

Nineth, proportionality must guide secure exchange design. Overly restrictive systems may discourage meaningful participation, while overly permissive systems undermine trust. The protocol should be calibrated to the sensitivity of information shared.

Finally, trust itself is part of secure exchange. In most cases, PPPs are mostly about trust and nimble exchange based on mutual understanding of common needs. Therefore, for areas with lower risk exposure of information leaks, PPPs should allow nimble and proactive sharing.

In summary, secure data exchange protocols in a PPP require a layered approach: certified technical infrastructure, structured access governance, clear classification and purpose limitation, defined retention rules, audit mechanisms, incident response planning, legal reinforcement, and trained personnel. Technology enables security, but disciplined governance sustains it.

4. Roles and Responsibilities: Explicit Allocation

4.1 Responsibilities of Public Authorities

Public authorities entering a PPP carry specific responsibilities that go beyond convening and presiding meetings or receiving information. Because they hold legal authority, enforcement powers, and strategic oversight, their role shapes both the credibility and the fairness of the partnership.

First, public authorities must provide strategic direction. This means clearly articulating the risk priorities that justify the PPP's existence. They should present documented risk assessments, emerging threat analyses, and sectoral vulnerabilities in a structured and accessible manner. Without this strategic framing, private institutions may not understand the broader threat landscape or the rationale behind certain thematic focuses.

Second, authorities must provide contextual intelligence where legally permissible. While sensitive operational details may be restricted, authorities should share declassified or sanitised insights about trends, methodologies, and risk evolution. Private institutions cannot calibrate monitoring systems effectively if they operate without threat context. Sharing aggregated patterns, behavioural indicators, and typology developments strengthens detection capacity without compromising investigations.

Third, public authorities must clarify expectations. This includes being explicit about what constitutes high-quality reporting, what investigative thresholds typically trigger action, and what deficiencies are commonly observed. Ambiguous expectations create defensive reporting behaviour and reduce the effectiveness of suspicious transaction systems.

Fourth, authorities must provide structured feedback. One of the most common frustrations in AML/CFT frameworks is the perceived lack of feedback after reporting. Within a PPP, feedback should be institutionalised. This does not require sharing sensitive investigative details, but it does require communicating whether reporting patterns are useful, misaligned, or in need of refinement. Feedback transforms reporting from a compliance obligation into a risk partnership.

Fifth, public authorities must ensure proportionality and fairness. They must avoid favouring particular institutions or creating perceptions of privileged access. Participation should not translate into regulatory leniency or enforcement advantage. Equal treatment safeguards trust and prevent market distortion.

Sixth, authorities must protect confidentiality rigorously. Information received from private institutions must not be disclosed beyond legal boundaries. Any breach of confidentiality can irreparably damage trust and discourage future cooperation. Information exchanged for the purposes of the PPP work should stay within the PPP, unless specific authorisation for

further dissemination is granted. This means that if a specific FIU unit is part of a PPP, further disclosure to other FIU departments should be provided only based on prior authorisation.

Seventh, authorities should coordinate internally. In many jurisdictions, FIUs, supervisors, law enforcement, and ministries operate with different priorities. If these bodies provide inconsistent signals within a PPP, credibility is weakened. Public sector coordination prior to PPP engagement is therefore essential.

Eighth, public authorities must avoid transferring investigative responsibility to private partners . While enhanced monitoring may be encouraged, private institutions are not substitutes for law enforcement. The PPP should not become a mechanism for informal tasking without legal safeguards.

Ninth, authorities must allocate sufficient resources. Convening, analysis, follow-up, and feedback require dedicated personnel. If public authorities lack analytical capacity or coordination support, the PPP will struggle to produce tangible outcomes.

Tenth, authorities must be transparent about limitations. There will be instances where operational sensitivity prevents full disclosure. Being clear about such limitations helps manage expectations and preserve trust.

Finally, public authorities should view the PPP as a two-way accountability mechanism. Just as private institutions are expected to enhance detection and compliance, authorities should also reflect on how PPP outputs inform supervisory focus, policy reform, and enforcement strategy.

In essence, the responsibility of public authorities within a PPP is not simply to lead, but to lead responsibly. They must provide strategic clarity, contextual intelligence, proportional expectations, structured feedback, internal coordination, resource commitment, and confidentiality safeguards. When these responsibilities are fulfilled explicitly and consistently, the PPP becomes balanced, credible, and sustainable.

4.2 Responsibilities of Private Sector Partners

Private sector partners entering a PPP do not participate merely as information providers or passive recipients of guidance. Their role is active, analytical, and operational. Because they sit at the frontline of financial transactions, closest to the ML/TF emerging risks and customer interaction, their contribution is central to the effectiveness of the partnership.

First, private institutions must commit to meaningful engagement. Participation should not be symbolic or reputational. Representatives attending PPP meetings must be sufficiently senior or technically empowered to influence internal monitoring frameworks, risk policies, and operational procedures. Without decision-capable representation (or at least, direct access to such), discussions will not translate into action.

Second, institutions must share operational insights in good faith. Authorities benefit significantly from understanding how criminal schemes manifest in real transaction flows, as well as where monitoring systems struggle to identify risk. Controls and working methods are not always perfect.

Third, private partners must contribute to typology development. Rather than relying solely on public authorities for risk narratives, institutions should actively share patterns observed internally. Collective understanding improves when multiple institutions compare experiences and identify common threads.

Fourth, institutions must assess and, where appropriate, adjust internal controls based on PPP outputs. Participation implies a willingness to refine transaction monitoring scenarios, update risk indicators, improve reporting quality, and enhance staff training in response to shared insights. A PPP loses credibility if discussions do not lead to internal action.

Fifth, private sector partners must ensure proportional and lawful use of shared intelligence. Information received through the PPP should inform risk assessment and compliance measures, but it must not lead to automatic de-risking or indiscriminate account closures without internal evaluation. Institutions remain responsible for applying independent judgment within legal frameworks.

Sixth, confidentiality obligations must be strictly respected. As already mentioned, private sector institutions must ensure that access is limited to authorised personnel and that internal dissemination follows agreed protocols.

Seventh, partners must allocate adequate resources. Effective participation requires analytical capacity, preparation time, and follow-up implementation. This may involve dedicating specific compliance or financial intelligence staff to PPP engagement. In many instances, it is even expected that the private sector has more resources to dedicate but this shouldn't be the norm and if so, it should be based on a clear prior agreement in the PPP. Normally, reciprocity should apply in all cases. This means that more capacitated institutions should contribute with more resources.

Eighth, private partners should provide structured feedback to authorities. If certain red flags generate excessive false positives, or if reporting expectations are unclear, institutions should communicate this openly. Constructive feedback strengthens proportionality and improves regulatory clarity.

Ninth, institutions must avoid competitive misuse of PPP information. The partnership is designed for systemic risk mitigation, not commercial advantage. Shared insights should not be used to gain competitive intelligence or market leverage.

Tenth, private sector partners must embrace long-term commitment. PPPs generate value over time through accumulated trust and iterative improvement. Short-term participation

without sustained engagement limits strategic impact. Of course, it isolated cases, PPPs could be established or partners engaged for individual (short-term) tasks or purposes.

Capacity asymmetry is an inherent feature of PPs. Not all participants operate with equal analytical resources, technological sophistication, staffing levels, or institutional maturity. Large financial institutions may have dedicated financial intelligence teams, advanced transaction monitoring systems, and internal data science capacity. Smaller institutions, fintech companies, or non-financial obliged entities may operate with limited compliance staff and constrained technical infrastructure.

If not carefully managed, capacity asymmetry can create imbalance within the PPP. Discussions may become dominated by larger or more sophisticated participants. Their analytical depth and technical vocabulary may unintentionally marginalise smaller actors. Over time, these risks creating a "two-speed" partnership where only a subset of institutions meaningfully shape outputs. Red flags or typology guidance developed in a resource-rich environment may be impractical for smaller entities to implement. Detection scenarios requiring complex data aggregation or advanced analytics may be unrealistic for institutions with limited infrastructure. Participation burden may become uneven. Frequent meetings, analytical preparation, or technical platform engagement may be manageable for large institutions but strain smaller participants.

Asymmetry may also create reputational or supervisory anxiety. Smaller institutions may hesitate to share challenges openly if they fear exposing resource limitations. Addressing capacity asymmetry requires deliberate design choices.

One approach is tiered participation. The PPP can allow varying levels of engagement depending on risk exposure and institutional capacity. For example, strategic discussions may be open to a broad range of participants, while highly technical working groups may involve institutions with relevant expertise.

Another approach is proportional implementation guidance. When developing red flags or typologies, outputs should include scalable options. For instance, guidance may describe a basic monitoring approach suitable for smaller institutions and an advanced analytical option for larger entities. This prevents guidance from becoming exclusionary.

Capacity-building components can also be integrated into the PPP. Joint training sessions, shared typology briefings, or simplified detection templates can support smaller participants. In this way, the PPP becomes not only a coordination platform but also a knowledge equaliser. Secure technology platforms should also be calibrated to accessibility. Overly complex systems may discourage participation. User-friendly interfaces and structured templates can lower entry barriers.

Resource pooling is another option. In some models, analytical tasks may be led by institutions with greater capacity, with outputs shared across the partnership. However, this must be carefully governed to avoid creating dependency or perceived hierarchy.

Importantly, transparency about capacity constraints should be normalised. PPP culture should allow participants to openly discuss operational challenges without reputational fear. This builds trust and enables realistic solutions.

Capacity asymmetry may also exist within the public sector. Smaller FIUs or supervisory authorities may face resource limitations in engaging in transnational or technologically advanced PPP models. Therefore, design must consider not only private-sector disparities but also public-sector constraints.

In essence, the responsibility of private sector partners is to participate actively, contribute substantively, implement responsibly, protect confidentiality rigorously, allocate resources adequately, and engage in sustained and constructive collaboration. When these responsibilities are met, the PPP evolves from a regulatory forum into a genuine partnership for financial system integrity.

5. Building and Sustaining Trust

Building and sustaining trust within a PPP goes far beyond regular meetings or structured agendas. While predictability creates stability, trust is ultimately built through consistent behaviour, fairness, and demonstrated value over time.

First, clarity of roles and boundaries is fundamental. Trust weakens when institutional mandates are blurred or when one partner appears to overstep its authority. It creates competition and erodes trust.

Second, fairness and equal treatment across the private and public part are essential. If certain institutions receive preferential access to intelligence, informal regulatory advantages, or disproportionate influence over the PPP's agenda, other participants will disengage. Trust grows when participation is structured transparently and applied consistently. If the PPP is divided into public and private partners, this also undermines trust.

Third, transparency of process strengthens confidence. Participants should understand how decisions are taken, how priorities are selected, and how outputs are validated. Even when not all information can be disclosed, explaining why certain constraints exist preserves institutional confidence.

Fourth, demonstration of tangible outcomes is critical. Trust is reinforced when participants see that discussions lead to measurable improvements such as clearer red flags, improved

reporting quality, or faster disruption of criminal schemes. Without visible impact, enthusiasm erodes over time.

Fifth, responsible handling of sensitive information is indispensable. One breach of confidentiality can undo years of relationship-building. Strict enforcement of third-party rules, immediate response to any misuse, and transparent communication in case of incidents protect the partnership's integrity.

Sixth, balanced reciprocity builds mutual respect. Trust diminishes if one side consistently contributes more than it receives. Reciprocity does not mean identical contributions, but it does mean that both public authorities and private institutions perceive value and effort on both sides.

Seventh, institutional continuity supports long-term trust. High turnover of representatives can weaken relationships and institutional memory. Whenever possible, stable representation should be encouraged, with structured handover procedures when changes occur.

Eighth, openness to constructive disagreement strengthens maturity. PPPs should allow space for candid discussion about implementation challenges, legal uncertainties, or supervisory expectations, even room for disagreement and honest brainstorming for solutions. A culture that tolerates respectful disagreement is more resilient than one that avoids difficult conversations.

Ninth, proportionality in expectations is crucial. If public authorities impose unrealistic demands, or if private institutions expect privileged treatment, trust deteriorates. Clear communication of limitations and constraints on both sides prevents misaligned expectations.

Tenth, cultural understanding matters. Public and private sectors operate under different incentive systems, risk appetites, and accountability structures. Recognising and respecting these differences reduces friction and fosters empathy.

Finally, trust is cumulative. It develops through repeated cycles of cooperation: shared analysis, responsible information exchange, constructive feedback, and observable results. It cannot be mandated, but it can be structured and nurtured through consistent governance, fairness, competence, and transparency.

In essence, predictability lays the foundation, but sustained trust requires fairness, reciprocity, clarity, competence, transparency, confidentiality discipline, realistic expectations, and visible impact. When these elements are consistently present, a PPP becomes resilient even under pressure or institutional change.

6. Information Exchange Models

The features of all three models can be easily determined by the information provided in the text above. Therefore, here the Guidance only briefly outlines the three potential PPP models.

6.1 Strategic-Only Model

Suitable for jurisdictions with legal constraints. Provides shared awareness but limited operational coordination.

The strategic model focuses on the exchange of high-level risk information, including typologies, emerging trends, and sectoral vulnerabilities. Information is typically anonymized or aggregated and does not involve operational details about specific individuals or entities.

Strategic PPPs usually have the greatest outreach (e.g. through typology papers) and their time-to-market is usually also the longest to create. In addition, the time necessary for all engaged parties to notice the effect of the PPP is also usually longer than compared to the other two types.

This model is often easier to establish because legal and confidentiality constraints are less complex. It also allows the partnership to engage a broader range of stakeholders, including institutions that may not be directly involved in operational ML/TF investigations.

Because the outputs of a strategic PPP are generally less sensitive, they can often be disseminated more widely across the financial sector and other relevant partners, including the general public (e.g. in some fraud-related cases). This allows the partnership to reach a broad audience and improve general awareness of ML/TF and predicate crime risks.

However, strategic outputs may require longer preparation cycles, as typology development, validation, and sectoral consultation can take time. As a result, the time-to-market for outputs may be slower compared to more operational models.

In practice, the strategic model is particularly useful in the early stages of a PPP or where legal constraints limit operational information sharing.

6.2 Operational Case-Based Model

Enables targeted intervention. Requires stronger legal clarity and governance safeguards.

The operational model involves targeted exchanges of operational data and even intelligence, potentially including information about specific individuals, entities, networks, or transaction patterns linked to ML/TF and predicate crime risks.

Operational PPPs provide the most direct valuable input and the shortest time-to-market, but they are also covering the most limited target group of partners (as operational information should only be shared with those parties which are affected).

Because the objective is to support real-time or near-real-time risk mitigation, the operational model typically emphasises speed of response. Information can be shared rapidly in order to allow institutions to detect suspicious activity, prevent asset dissipation, or support ongoing investigations.

The time-to-market of outputs is therefore usually very short, often measured in days or even hours in urgent cases.

However, operational exchanges must be carefully governed due to their sensitivity. Legal frameworks, strict access controls, and clearly defined safeguards are essential. Participation is therefore usually limited to a smaller group (PPP sub-groups) of trusted and relevant institutions and authorities, and the dissemination of outputs is typically restricted.

While the outreach of operational PPPs is narrower, their impact can be highly targeted and immediate.

6.3 Hybrid Model

Combines strategic insight with operational flexibility. Most adaptable in dynamic risk environments.

Many mature PPPs adopt a hybrid approach, combining elements of both strategic and operational cooperation.

Under this model, different layers of cooperation coexist:

- Strategic analysis and typology development may be shared more broadly across all partners.
- Tactical alerts or behavioural patterns may be shared with a more limited and relevant group (sub-group) of institutions.

- Highly sensitive operational intelligence may remain restricted to specific authorised participants.

The hybrid model balances speed, impact, and inclusiveness. Strategic outputs provide broad preventive value, while operational exchanges allow rapid responses to emerging threats.

As a result, both time-to-market and outreach can be calibrated according to the sensitivity of the information and the objectives of the partnership.

7. Technology-Enabled PPPs

Technology-enabled PPPs represent an evolution from dialogue-based cooperation to structured, scalable, and data-driven collaboration. Technology does not replace trust or governance, but it significantly enhances speed, analytical depth, auditability, and security when properly designed.

At the most basic level, technology enables secure communication. Encrypted collaboration platforms, certified secure networks, and controlled-access portals allow participants to exchange sensitive information without relying on unsecured email or fragmented channels. However, the true value of technology in PPPs goes far beyond secure messaging.

One important dimension is structured information management. Digital platforms can host shared typology repositories, red flag libraries, and documented guidance notes. This ensures institutional memory and consistency, particularly when participants change roles. A centralised knowledge base reduces duplication and strengthens continuity.

A second dimension is analytical augmentation. Technology can support joint risk analysis without requiring full data pooling. For example, privacy-enhancing technologies (PETs) such as secure multi-party computation or federated learning allow institutions to identify shared patterns across datasets without exposing raw data. This preserves confidentiality while enabling collective intelligence generation.

A third dimension is automation of information flows. In more advanced PPPs, structured templates can be integrated into digital systems, allowing standardised submission of risk indicators or structured alerts. Automated logging, tagging, and categorisation improve traceability and reduce administrative burden.

A fourth dimension is auditability and accountability. Technology-enabled platforms can maintain detailed access logs and activity records. This strengthens compliance with data protection obligations and reassures participants that sensitive intelligence is not misused.

A fifth dimension is scalability. As PPPs grow to include additional institutions or thematic working groups, manual coordination becomes inefficient. Secure digital ecosystems allow structured access rights, thematic sub-groups, and tiered information-sharing layers without compromising security.

Artificial intelligence can also play a supportive role. AI tools may assist in identifying patterns within shared typology data, clustering behavioural indicators, or detecting emerging trends across anonymized contributions. However, AI use must be governed carefully and remain human-driven. Transparency, explainability, and human oversight remain essential. Technology should enhance professional judgment, not substitute it.

Technology also enables real-time or near-real-time cooperation. In situations such as sanctions evasion or emerging fraud schemes, delays in information exchange reduce effectiveness. Secure platforms capable of rapid updates and controlled alert dissemination significantly enhance preventive capacity.

However, technology introduces new risks. Cybersecurity vulnerabilities, over-reliance on automated analysis, and unequal technological capacity among participants must be addressed. PPP governance should therefore include cybersecurity standards, periodic system audits, and clear rules on acceptable technological use.

Importantly, technology should be proportionate to the maturity of the PPP. Early-stage partnerships may begin with secure communication and structured documentation before advancing toward privacy-enhanced analytics or AI-supported collaboration. Overly ambitious technological design at an early stage can overwhelm institutional capacity and undermine trust.

Importantly, interpretative guidance from competent authorities on the use of technology for specific tasks – such as data protection, can often achieve clarity more quickly. Moreover, in the case of operational PPPs, early engagement with data protection authorities can prevent future conflict. Alignment between AML/CFT obligations and data protection requirements is essential. Clarifying lawful processing bases, proportionality standards, and data minimisation principles strengthens both legality and perceived legitimacy of the PPP. As mentioned above, technology can play significant role to support these objectives.

Finally, technology must serve clearly defined objectives. It is not the digital sophistication of a PPP that determines its success, but whether technology meaningfully enhances secure exchange, analytical depth, responsiveness, and accountability.

In essence, a technology-enabled PPP is not simply digitised cooperation. It is a structured, secure, and scalable ecosystem that strengthens collective intelligence generation while respecting legal safeguards and institutional autonomy.

8. Ensuring Nimbleness

Ensuring nimbleness is one of the distinguishing strengths of PPPs. Unlike formal legislative or treaty-based mechanisms, PPPs can react more quickly to emerging risks, evolving criminal methodologies, and geopolitical developments. However, adaptability must be structured and governed. Without clear frameworks, “flexibility” may become unpredictability.

Nimbleness matters because ML/TF and predicate crimes evolve faster than policy cycles. New sanctions regimes, emerging technologies such as decentralised finance, synthetic identity fraud, or cross-border layering schemes can materialise rapidly. A PPP must be capable of adjusting priorities, creating temporary task groups, or issuing rapid guidance without waiting for lengthy institutional processes.

To maintain structured adaptability, several mechanisms are important.

First, periodic strategic reassessment should be institutionalised. At least annually, the PPP should formally review whether its priorities still reflect current risk realities. This review should incorporate FIU intelligence trends, supervisory findings, enforcement outcomes, and private sector observations. The purpose is not to redesign the partnership every year, but to confirm or recalibrate focus.

Second, crisis-response protocols should be predefined. In urgent situations, such as major sanctions developments, terrorist financing alerts, or emerging fraud waves, the PPP should be able to convene rapidly, share contextual intelligence, and issue coordinated guidance. Having pre-agreed procedures for emergency engagement prevents confusion and delays.

Third, working group structures should be modular. The PPP should allow creation of temporary thematic groups that can be dissolved once objectives are achieved. Permanent structures should not become bureaucratic layers that resist change. Sunset clauses for working groups encourage efficiency and prevent institutional inertia.

Fourth, governance flexibility must coexist with accountability. Any change in priorities, scope, or information-sharing model should be formally documented and approved by the steering layer. This ensures that adaptation remains transparent and legally grounded.

Fifth, feedback mechanisms should feed directly into adaptation. If red flags prove ineffective, if reporting quality does not improve, or if certain themes lose relevance, adjustments should follow. A PPP that cannot modify its outputs risks becoming outdated.

Sixth, inclusiveness should evolve with risk. As new sectors become exposed, such as fintech platforms, VASPs, or non-financial gatekeepers, the PPP should have mechanisms to invite new participants proportionately. Controlled expansion ensures relevance while preserving security.

Seventh, proportional technological evolution supports nimbleness. As trust and maturity grow, the PPP may gradually integrate more advanced analytical tools or secure exchange mechanisms. This phased approach prevents technological overreach.

Eighth, leadership continuity supports adaptive stability. While adaptation is necessary, the partnership should maintain stable governance principles. Core commitments, such as confidentiality, proportionality, fairness, legal compliance must remain constant even as operational focus shifts.

Nimbleness should therefore be understood as structured agility. It is the ability to respond quickly within predefined governance boundaries. It requires clear decision-making pathways, documented processes for change, accountability for modifications, and respect for legal safeguards. Nonetheless, this nimbleness should be aligned with the domestic and supranational (if existing) AML/CFT strategies.

In essence, a nimble PPP is not one that constantly reinvents itself, but one that can recalibrate efficiently without destabilising trust or compromising governance. Adaptability becomes sustainable only when it is disciplined, transparent, and aligned with documented risk priorities.

9. Measuring Effectiveness

Measuring effectiveness in a PPP is essential for legitimacy, sustainability, and improvement. A PPP involves institutional trust, allocation of resources, and often sensitive cooperation. Without structured evaluation, it becomes difficult to justify continued engagement or demonstrate value. Effectiveness measurement serves several purposes.

First, it demonstrates impact. Senior leadership in both public and private institutions will expect evidence that the PPP contributes to improved ML/TF and predicate crime detection, disruption, or risk mitigation. In many instances, this enhanced effectiveness, means better resource optimization.

Second, it reinforces accountability. If objectives were defined at the outset, measuring performance ensures that those objectives are taken seriously and periodically reviewed.

Third, it supports adaptation. Measurement is not merely about validation, but it reveals gaps and areas requiring adjustment.

A practical approach to measuring effectiveness requires clarity about what the PPP is designed to achieve. Metrics must be aligned with objectives and proportionate to the partnership's maturity level. Effectiveness can be assessed across four interconnected dimensions: operational impact, strategic impact, system improvement, and partnership health.

Operational impact refers to tangible improvements in detection and disruption. Examples include:

- Improved quality of suspicious transaction reports in targeted thematic areas. This may be assessed through structured FIU feedback indicating greater relevance, clearer narratives, or stronger linkage to typologies discussed within the PPP.
- Reduced response times in urgent information exchanges, particularly in operational intelligence contexts.
- Increased identification of shared red flags across institutions, leading to earlier detection of coordinated networks.
- Evidence that PPP-related intelligence contributed to asset freezing, investigation initiation, or disruption of specific schemes.

It is important to avoid over-attribution. A PPP may contribute to improved outcomes without being the sole cause. The goal is to identify plausible linkage, not claim exclusive credit.

Strategic impact refers to systemic improvements in risk awareness and mitigation. This may include:

- Integration of PPP findings into National Risk Assessments or sectoral risk documents.
- Alignment between supervisory findings and typologies identified within the PPP.
- Updates to compliance guidance reflecting jointly developed red flags.
- Enhanced consistency in risk interpretation across institutions.

Strategic indicators often manifest over a longer timeframe and require qualitative assessment.

System improvement indicators focus on process enhancement. For example:

- Better alignment between reporting entities and FIU expectations.
- Reduced volume of low-value reporting in favour of higher-quality submissions.
- Improved calibration of transaction monitoring systems following PPP guidance.
- Greater clarity in supervisory communication.

These improvements reflect maturity of cooperation rather than single-case outcomes.

Partnership health indicators are equally important. Even a technically successful PPP can deteriorate if trust weakens. Health indicators may include:

- Consistency of participation across institutions.
- Engagement levels during meetings.

- Implementation follow-through on agreed actions.
- Feedback from participants regarding perceived value.
- Balance in contributions between public and private sectors.

Without monitoring partnership health, long-term sustainability may be compromised.

In designing measurement frameworks, proportionality is essential. Early-stage PPPs may focus on qualitative indicators such as improved dialogue and shared understanding. More mature PPPs can incorporate quantitative metrics, structured performance reviews, and documented outcome tracking.

Measurement should also be periodic but not overly burdensome. An annual structured review conducted by the strategic steering layer can assess:

- Whether the PPP addressed its defined risk priorities.
- Whether tangible improvements occurred.
- Whether adjustments in governance, scope, or resources are required.

Transparency in performance reporting strengthens institutional buy-in. When partners see documented evidence of progress, commitment deepens. When weaknesses are acknowledged and addressed constructively, trust grows.

Finally, measuring effectiveness should not become punitive or overly compliance driven. The objective is collective improvement, not performance ranking among institutions. The PPP is a shared instrument of systemic integrity, and measurement should reinforce collaboration rather than competition.

In essence, effectiveness measurement provides legitimacy, drives adaptation, strengthens trust, and secures long-term political and institutional support. Without it, even a well-designed PPP risks gradual erosion of relevance and engagement. These are only few examples, but assessment models can differ based on the specific particularities of the PPP.

10. The Future of PPPs

The future of PPPs will be shaped by the increasing complexity and transnational character of ML/TF and predicate crimes. Money laundering, terrorist financing, sanctions evasion, professional enablers, and technology-enabled fraud schemes operate across borders, sectors, and asset classes. Criminal networks exploit regulatory fragmentation, legal asymmetries, and institutional silos. In this environment, nationally confined cooperation models may no longer be sufficient.

Transnational PPPs are already emerging. The European context provides a clear example (with EFIPPP), where high levels of legal harmonisation, supranational coordination, and institutional integration make cross-border PPP models more feasible. However, the existence of transnational PPPs within the EU does not mean that such models are limited to highly integrated jurisdictions. Similar approaches are possible elsewhere, provided that certain enabling conditions are met.

The core question is not whether transnational PPPs are possible, but how they are structured and governed. Therefore, the future of PPPs is likely to be **multidimensional**.

The Egmont Secure Web (ESW) offers a reliable mechanism for FIUs to exchange experiences, identify counterparts with established PPP frameworks, and explore opportunities for cooperation and knowledge-sharing. However, FIUs may use the ESW only in accordance with the Egmont Group Principles for Information Exchange between FIUs. Any exchange intended to support a PPP should therefore be clearly identified in the request for information.

At the domestic level, PPPs will increasingly become embedded components of national AML/CFT frameworks rather than experimental initiatives. They will move from dialogue platforms to structured risk management mechanisms that generate typologies, refine red flags, improve reporting quality, and support measurable disruption outcomes.

At the cross-border level, PPPs may (is likely to) develop around specific shared threats rather than broad, general cooperation. Transnational PPPs are most viable when they focus on risks that are inherently international in nature, such as sanctions evasion networks, virtual asset misuse, large-scale cyber-enabled fraud, TBML, large terrorist groups (from the perspective of their financing), or professional laundering networks operating across jurisdictions.

Large (multinational) financial institutions might already have a transnational view on specific risks related to their activity. Therefore, this may require a more targeted steps to be taken by the public sector, in order to catch up, especially in jurisdictions with more advanced and tightly connected economic and financial markets.

Such cross-border PPPs require a credible convening structure. This may be a supranational authority, a regional body, or a coalition of jurisdictions with shared exposure to particular threats. The presence of a trusted convenor increases legitimacy, ensures governance consistency, and facilitates resource pooling.

One of the most important future questions concerns the route of information exchange.

Possibly, in some of the models, information exchange is primarily channelled through FIUs. FIUs already operate under established international cooperation principles and secure channels, and they provide a legally structured pathway for financial intelligence exchange. This model offers clarity, established safeguards, and familiarity. However, if overly

centralised, it may limit the speed or multidimensionality of collaboration, also due to the strict dissemination requirements.

Another possibility is that the information exchange takes place in a more holistic framework that involves FIUs, supervisors, law enforcement authorities, and private institutions within a structured and governed environment. This approach will allow richer situational awareness and faster alignment between detection, supervision, and disruption. However, it requires stronger governance, clearer legal frameworks, and enhanced data protection safeguards. Diagonal international cooperation between (non-)counterparts can be the typical way to explain such cooperation.

A hybrid approach may represent the most sustainable future architecture. Under such a model, information exchange is tiered according to sensitivity and purpose. Strategic typologies and sectoral risk indicators may circulate broadly within the PPP framework. Tactical alerts or emerging behavioural patterns may be shared under controlled access. Highly sensitive operational intelligence, such as targeted identifiers, may remain channelled through established FIU or law enforcement pathways while being complemented by contextual briefings within the PPP. This tiered structure allows PPPs to remain both effective and legally defensible.

The future maturity of PPPs will also require deeper integration with the broader AML/CFT apparatus. PPP outputs should inform National AML/CFT Strategies and Risk Assessments, policy-making initiatives, and other AML/CFT priorities. Conversely, supervisory findings, investigative outcomes, and FIU intelligence should feed back into PPP discussions. Without such integration, PPPs risk becoming parallel structures rather than embedded components of the ML/TF and predicate crime ecosystem.

Technology will play an increasing role in enabling cross-border collaboration. Secure digital platforms, audit trails, structured templates, and privacy-enhancing technologies can reduce legal friction and strengthen trust. However, technological sophistication must be matched by governance maturity. Trust, clarity of mandate, proportionality, and legal certainty remain foundational.

Ultimately, the future of PPPs is not defined by a single model, but by their capacity to evolve into coordinated, layered, and adaptive cooperation mechanisms. As ML/TF and predicate crimes become more interconnected and technologically advanced, PPPs must move beyond informal dialogue toward structured, integrated, and multidimensional collaboration frameworks.

Their effectiveness will depend on their ability to balance speed with safeguards, flexibility with governance, national priorities with cross-border realities, and innovation with legal certainty. In a ML/TF and predicate crime environment of growing complexity, the maturity and integration of PPPs will become a critical component of systemic resilience.

Finally, this Guidance also acknowledges the growing role of private-to-private cooperation (P2P). P2P mechanisms can complement traditional PPP arrangements by facilitating information sharing, risk identification, and collective responses among private-sector entities facing common threats. In sectors where information fragmentation remains a challenge, enhanced collaboration among private-sector participants may contribute to a more comprehensive understanding of risks and improve preventive and detection capabilities.

11. The Role of FIUs

FIUs occupy a structurally unique position within PPPs. They sit at the intersection of reporting entities, supervisory authorities, and law enforcement bodies. They receive financial intelligence from the private sector, analyse it, and disseminate it for investigative or (sometimes) supervisory action. At the same time, they contribute to strategic risk assessments and inform national AML/CFT policy development.

In an evolving PPP environment, the role of FIUs is therefore pivotal.

First, FIUs act as intelligence integrators. They are often the only actors with a system-wide overview of suspicious activity reports across sectors. This aggregated visibility allows them to identify cross-institutional patterns that no single private institution can detect. Within a PPP, FIUs can transform fragmented reporting into structured typologies, contextual threat briefings, and prioritised risk themes.

Second, FIUs serve as a trusted intermediary between the private sector and law enforcement. In many jurisdictions, direct operational interaction between reporting entities and investigative authorities may be limited or legally sensitive. FIUs provide a structured channel through which financial intelligence can flow securely and lawfully. This intermediary function becomes even more important in transnational contexts, where FIU-to-FIU cooperation frameworks are already established.

Third, FIUs contribute to supervisory alignment. By analysing reporting quality and emerging patterns, they can provide feedback that informs supervisory focus and inspection strategies. Conversely, supervisory findings regarding control weaknesses can inform FIU strategic analysis. Within a PPP, FIUs help ensure that operational intelligence, compliance expectations, and supervisory priorities are mutually reinforcing rather than fragmented.

Fourth, FIUs are well positioned to anchor risk-based prioritisation. Because they assess incoming intelligence across the system, they can identify which typologies or sectors present the most immediate or systemic risk. This enables PPPs to focus on material threats rather than anecdotal concerns.

However, the evolving PPP landscape also presents structural challenges for FIUs.

FIUs typically operate under resource constraints. Analytical capacity is finite. Staff are often heavily engaged in case processing and dissemination responsibilities. Expanding PPP engagement must therefore be carefully prioritised. If not structured properly, PPP participation could risk overextension of core mandates.

For this reason, FIUs in a mature PPP environment must be exceptionally targeted and efficient. They should focus their engagement on areas where they provide unique value: aggregated intelligence insight, cross-sectoral pattern detection, strategic prioritisation, and structured feedback. Routine administrative coordination or functions that can be performed by other actors should not overburden FIU capacity.

In this sense, often the role of FIUs can be described as primus inter pares (first among equals) within the PPP architecture. They do not dominate the partnership, nor do they substitute for supervisory or investigative mandates. However, their integrative and intelligence-centric position gives them a coordinating and directional function.

This leadership must be exercised with balance. FIUs should avoid over-centralisation of the PPP, which could limit multidimensional cooperation. At the same time, they should ensure that operational intelligence exchanges remain legally grounded and proportionate.

In transnational PPP environments, the FIU role may become even more important. Established FIU-to-FIU cooperation channels, secure exchange principles, and shared professional standards provide a stable backbone for cross-border collaboration. At the same time, FIUs must adapt to more holistic and diagonal cooperation models that include supervisors, law enforcement, and private partners within structured governance frameworks.

Ultimately, the effectiveness of FIUs in the future PPP ecosystem will depend on their ability to combine analytical excellence, strategic prioritisation, operational prudence, and adaptive governance. They must remain intelligence-driven, legally disciplined, technologically aware, and partnership-oriented.

In a ML/TF and predicate crime environment of increasing complexity, FIUs are not merely participants in PPPs, but they are structural enablers. Their challenge is to lead without dominating, to coordinate without overextending, and to prioritise ruthlessly in order to deliver maximum systemic value with limited resources.

EGMONT GROUP

OF FINANCIAL INTELLIGENCE UNITS

www.egmontgroup.org

About the IEWG

Considering the mandates and activities of other working groups, the IEWG aims to increase the quality and quantity of timely information exchanges between FIUs based on operational and strategic analysis. Improving information exchanges will facilitate and enhance FIUs' adherence to international standards. In addition, the IEWG benefits from the expertise of its members, which contributes significantly to the working group's objectives.