

Cross-border AML data sharing

Legal hurdles, regulatory evolution,
strategic implementation pathways



Crisil Integral IQ analytical contacts

Mudit Goel

Head of India's Markets and InvestOps Practice

mudit.goel@crisil.com

Abhyanshu Bhardwaj

Manager, Financial Crime Compliance

abhyanshu.bhardwaj@crisil.com

Varun Shah

Manager, Financial Crime Compliance

varun.shah@crisil.com

Breaking down borders

Money laundering is taking place across borders and with unprecedented speed and complexity. Yet anti-money laundering (AML) regimes remain fragmented, often limited by national privacy and secrecy rules.

Regulators worldwide are working to recalibrate laws and frameworks to encourage cross-border AML data sharing while preserving data protection standards.

The goal of these changes is not only compliance but also to empower financial institutions to better identify risks, reduce costs, and strengthen systemic resilience against financial crime.

This paper examines regulatory drivers, institutional benefits, legal barriers, and process-oriented solutions to align AML obligations with effective cross-border information sharing.



Borderless finance, boundless risk

Cross-border AML data sharing can help forge operational and regulatory solutions for better networking to prevent suspicious activities.

Laundering networks exploit jurisdictional gaps, operating seamlessly across multiple markets where regulators and institutions are constrained by national boundaries. No single regulator or institution can capture the full picture in isolation; effectiveness requires a collective, coordinated approach.

Hence, cross-border AML data sharing is not just a regulatory aspiration, but a necessity in today's borderless financial system.

The global nature of laundering poses significant challenges. Complex schemes such as under- and over-invoicing conceal illicit funds within legitimate trade flows, often requiring cooperation between customs, banks and regulators in multiple jurisdictions. Correspondent banking exposure is another risk, where banks facilitating cross-border payments face risks that are invisible if viewed only at a local level.

Global data exchange is essential to uncover hidden risks. The speed and global reach of cryptocurrencies and digital exchanges enable funds to move across continents in seconds, often outpacing regulators' ability to respond.



The regulatory purpose behind reforms is to close blind spots, ensuring institutions can access, process and exchange AML-critical data across jurisdictions—without becoming paralyzed by conflicting national laws.

FATF Recommendations 37-40 emphasize the need for strong mechanisms of international cooperation and intelligence exchange. The European Union AMLD6 and the upcoming AML Authority (AMLA) are designed to eliminate intra-EU fragmentation and establish a single supervisory approach. The US AML Act of 2020 expands safe harbors to encourage institutions to share intelligence without fear of liability. Asian regulators such as MAS (Singapore) and HKMA (Hong Kong) are pioneering group-wide oversight frameworks and piloting privacy-preserving technologies to reconcile compliance with confidentiality.



A strategic opportunity for financial institutions

For financial institutions, aligning with cross-border AML reforms is more than a compliance obligation; it is a strategic opportunity. By embracing these frameworks, institutions can strengthen detection capabilities, reduce operational costs, and position themselves as trusted partners to regulators and clients alike. Linking transaction data across jurisdictions enables holistic customer risk profiling, revealing patterns such as layering and structuring that would be invisible at a single-market level. Centralized or standardized systems eliminate duplication across subsidiaries, allowing compliance teams to focus on analysis rather than repetitive reporting. Standardized reporting templates simplify regulatory engagement, particularly for multinational banks.

High-profile scandals such as those involving Danske Bank, Swedbank and Wirecard demonstrate the cost of cross-border failures. Institutions that adopt stronger data-sharing practices reduce the likelihood of similar crises. Proactive collaboration builds goodwill with supervisors, often leading to reduced scrutiny. Participation in cross-border public–private partnerships (PPPs) elevate institutions from being seen as mere rule-followers to being strategic partners in crime prevention.



Legal and operational hurdles

Despite the clear benefits, implementation remains highly complex. Legal, regulatory and technical barriers continue to limit the seamless sharing of AML data. Institutions must navigate these challenges with care, balancing legal obligations with operational needs. Frameworks such as the EU's GDPR and China's PIPL place strict controls on cross-border personal data transfers. While AML exemptions exist, their interpretation and application differ widely between jurisdictions. Even FATF-compliant jurisdictions often diverge on key definitions, such as beneficial ownership thresholds or suspicious transaction reporting requirements, creating friction for multinational banks.

Suspicious activity reports (SARs) remain tightly controlled; many jurisdictions prohibit their cross-border transmission, limiting their usefulness for global monitoring teams. Legacy IT infrastructure in many institutions is unable to support advanced data models, encryption frameworks or federated learning, leaving them ill-prepared for modern, privacy-safe sharing mechanisms.



Investing in strategic solutions

To unlock the benefits of cross-border AML data sharing, institutions and regulators must go beyond legal harmonization and invest in **practical, technology-driven and collaborative solutions**.

These strategic solutions offer a pathway to implementation that balances compliance with effectiveness.

Regulatory harmonization

- Establish explicit carve-outs in privacy laws for AML-related transfers
- Expand bilateral and multilateral adequacy agreements (e.g., EU-US frameworks) to provide clear legal bases for data sharing
- Use FATF peer reviews to ensure consistent exemptions and best-practice adoption across jurisdictions

Privacy-preserving technology deployment

- Federated learning allows institutions to detect suspicious patterns without sharing raw data
- Homomorphic encryption enables exchange of risk scores and analytics in a mathematically secure way
- Recognition of privacy-enhancing technologies by regulators as valid compliance evidence is critical to scaling up adoption

Group-wide monitoring frameworks

- Multinational institutions should implement unified AML policies recognized by both home and host regulators
- Subsidiaries can exchange red-flag indicators while minimizing unnecessary exposure of personal data
- Comprehensive audit trails ensure accountability and proportionality

PPPs with cross-border reach

- Extend domestic PPPs such as the UK's Joint Money Laundering Intelligence Taskforce or Australia's Fintel Alliance into regional and global coalitions
- Develop regulator-led cross-border financial intelligence sharing platforms
- Create case-specific agreements that enable rapid intelligence flows for emerging threats

Streamlined SAR information exchange

- Deploy encrypted, regulator-governed platforms for SAR data
- Pilot anonymized SAR typology exchanges to test effectiveness while mitigating legal risks
- Promote harmonized SAR reporting templates (e.g., FIU.Net, FATF formats) for greater global usability



Reimagining the future

In moving towards a truly global financial crime compliance framework, the future of cross-border AML data sharing requires more than just tactical solutions.

It needs a reimagined architecture that integrates paradigm shifts in regulatory thinking, foundational pillars for sustainable operations, and a forward-looking vision for what AML information ecosystems should evolve into.

This section explores these three dimensions, positioning them as complementary lenses rather than competing frameworks.

Paradigm shifts in cross-border AML data sharing

AML data sharing must transition from a check-box regulatory activity to a collective defense mechanism against global illicit financial flows. Compliance is not the end; it is the means toward preserving financial system integrity.

Current sharing models rely heavily on bilateral memoranda and agreements between financial intelligence units (FIUs). A paradigm shift toward multilateral, networked platforms will unlock faster dissemination of intelligence on suspicious activities across regions. Instead of guarding data as proprietary, financial institutions and FIUs must treat themselves as stewards of intelligence serving a higher public interest, subject to privacy-safe handling under laws such as the General Data Protection Regulation.

Today's AML data models are siloed. Harmonization through ISO 20022 taxonomies and FATF-driven frameworks is critical for building interoperable infrastructures that can talk across borders. Rather than waiting for red flags to trigger data sharing, institutions and regulators should build anticipatory models that leverage typology intelligence, real-time corridor risks and predictive analytics.

Foundational pillars of cross-border AML data sharing

Every intrusion into customer privacy for AML purposes must be grounded in legal legitimacy, such as FATF Recommendations, EU AML Directives or US PATRIOT Act provisions. This gives regulators and financial institutions the moral and legal cover to cooperate.

Data sharing intensity must align with risk exposure. A corridor with heavy trade-based money laundering threats justifies greater intelligence flows compared with low-risk corridors. The technical capacity to align data formats, standards and taxonomies is central. Without interoperability, even lawful data sharing collapses in practice. Sharing is ineffective without reciprocity guarantees. If one FIU provides suspicious transaction reports, others must match that transparency and provide feedback loops.

Criminal typologies evolve. AML data-sharing systems must accommodate new risks such as crypto, cyber-enabled fraud, and shadow banking typologies.

The future-state vision for AML information ecosystems

Supranational utilities backed by FATF, Egmont Group or regional coalitions can function as neutral, secure repositories of cross-border AML intelligence. Risk-based sharing zones where the level of intelligence exchange reflects real-time monitoring of corridor vulnerabilities (e.g., high-risk remittance routes vs low-risk banking corridors) can be established.

Artificial intelligence can be trained across borders without moving raw customer data, thereby preserving sovereignty while enabling shared risk models. True AML effectiveness requires fusion across finance, customs, tax, cyber and trade regulators. Data-sharing hubs should enable multi-agency cooperation. Data can remain within sovereign borders, but analytical outputs, such as risk scores, network insights and typologies, can be transmitted securely across jurisdictions.

This reconceptualization of AML data sharing moves the dialogue from tactical fixes to strategic re-architecture.

By embedding paradigm shifts, grounding practices in foundational pillars and projecting toward future-state ecosystems, regulators and financial institutions can co-create an information-sharing framework that is both compliant with domestic laws and effective in global financial crime prevention.

Implementing these solutions requires structured planning. Institutions must align legal, technical and governance frameworks to create sustainable models.

Process-driven roadmap for effective cross-border AML data sharing



Regulatory mapping: Maintain jurisdictional registers of AML vs privacy conflicts



Technology investment: Prioritize privacy-enhancing technologies, federated monitoring and secure platforms



Process integration: Connect local compliance to centralized hubs; define escalation for global red flags



Stakeholder engagement: Proactively join PPPs, industry groups and regulator dialogues



Governance and training: Build AML-first culture; train staff on new sharing models



Staying ahead

The evolution of AML regulation reflects a clear purpose: to equip institutions with the ability to combat money laundering in a borderless financial system.

For regulators, reforms aim to balance privacy with systemic integrity. For institutions, the benefits lie in improved detection, efficiency and reduced risk.

Financial institutions that proactively align with cross-border AML reforms, adopt advanced technologies and embed new processes will position themselves as leaders in compliance and as trusted partners in the global financial system.

About Crisil Integral IQ (formerly Global Research & Risk Solutions)

Crisil Integral IQ delivers solutions and actionable intelligence to top financial institutions, driving strategic transformation, risk optimization, and operational excellence. Our offerings across research, risk, lending, analytics and operations have empowered clients to navigate complex markets, mitigate risks and unlock new opportunities. Our domain expertise, innovative solutions, future-ready technologies such as AI and data science give clients the confidence to accelerate growth and achieve sustainable competitive advantage. Our globally diverse workforce operates in the Americas, Asia-Pacific, Europe, Australia and the Middle East.

For more information, visit IntegrallQ.Crisil.com

About Crisil

Crisil is a global, insights-driven analytics company. Our extraordinary domain expertise and analytical rigour help clients make mission-critical decisions with confidence.

Large and highly respected firms partner with us for the most reliable opinions on risk in India, and for uncovering powerful insights and turning risks into opportunities globally. We are integral to multiplying their opportunities and success.

Headquartered in India, Crisil is majority owned by S&P Global.

Founded in 1987 as India's first credit rating agency, our expertise today extends across businesses: Crisil Ratings, Crisil Intelligence, Crisil Coalition Greenwich and Crisil Integral IQ.

Crisil's global workforce operates in the Americas, Asia-Pacific, Europe, Australia and the Middle East, setting the standards by which industries are measured.

For more information, visit www.Crisil.com

Connect with us: [LinkedIn](#) | [Twitter](#)

Crisil Privacy

Crisil respects your privacy. We may use your personal information, such as your name, location, contact number and email id to fulfil your request, service your account and to provide you with additional information from Crisil. For further information on Crisil's privacy policy please visit <https://www.crisil.com/content/crisilcom/en/home/crisil-privacy-notice.html>.