Fraud and AML convergence:

# Closing the speed gap

# Foreword



**Allison Swagert**
Senior Technical Customer Advisor, SAS

Financial crime rarely stays inside the lines an organization draws around it. Fraud, money laundering and sanctions evasion are often interconnected, even when the teams, technologies and processes designed to detect them are not. Most institutions still route detection and investigation based on organizational boundaries: Fraud owns fraud, AML owns AML and sanctions owns sanctions. There are often historically justifiable reasons for this delineation. But when risk doesn't respect those same organizational charts, financial institutions need integrated decisioning frameworks that are based on risk context across the enterprise, not just the department.

The risks associated with siloed financial crime detection frameworks are bigger than ever. Criminal networks are growing more sophisticated, and emerging technologies are creating new avenues for financial crime. Real-time payment rails move money around the world faster than ever, while cryptocurrency can make the origin of funds more difficult to trace. At the same time, institutions must comply with ever-changing regulatory requirements and are facing stringent expectations to protect customers, manage risk and respond effectively to threats that no longer fit neatly within the remit of a single function.

Against this backdrop, the case for greater alignment between fraud and anti-money laundering is compelling. But convergence should not be mistaken for simply combining two functions or asking teams to develop a single end-to-end workflow. Fraud detection and AML compliance carry distinct mandates, goals, responsibilities and methodologies – and that distinction is worth preserving. The real opportunity is to connect them where doing so makes institutions more effective: across key data and shared intelligence, core technology and solutions, workflow touch points, extended investigation and decision-making.

> When we talk about an integrated FRAML approach, the biggest change isn't where decisions are made; it's how these decisions are informed, coordinated and used to manage risk at the enterprise level.

The research in this report shows where financial institutions are on that journey; it's clear that meaningful convergence is not an end state that looks the same for every organization. Institutions are beholden to different regulators, run on different operating models and technology landscapes, and carry different risks and priorities. The goal is not to impose or insist upon a single "correct" framework but rather to create the connections that allow each function to benefit from what the other knows while preserving the expertise and accountability each brings to the fight against financial crime.

Technology is critical, but technology alone will not close the gap. Institutions also need strong data foundations, clear governance structures, workflows and organizational alignment that allow information and insights to move to the people who need them when they need them.

Every decision comes with tradeoffs: financial risk, regulatory exposure, customer impact and operational cost. The real question isn't whether those tradeoffs exist but is rather how they're evaluated – achieving a positive ROI requires considering them all.

Integrated FRAML is what allows those tradeoffs to be evaluated together – not sequentially, not in silos, and not after the fact. It enables banks to assess fraud and compliance risk at the same time, using shared signals, common context and consistent decision logic. When investigations are prioritized based on a holistic view of risk, teams aren't forced to choose between reducing losses, meeting regulatory expectations, reducing operational burden or improving customer experience. They can do all four, with one coordinated, defensible rationale. That's the difference between managing alerts and genuinely managing financial crime risk.

The path toward greater convergence will be an evolution rather than an immediate transformation. The institutions that make meaningful progress will be those that look beyond organizational boundaries and focus on the shared objective behind both disciplines: understanding financial crime more completely and responding to it more effectively.

# Table of Contents

Summary and Key Insights ..... 3
Staying the Course Will Leave Institutions Behind ..... 5
Why the Fraud vs. AML Silo Exists, and Why It Shouldn't Be Retained ..... 6
Different Mandate, Different Regulators ..... 6
The Battlefield: Intensifying Pressures on All Fronts ..... 8
Silos Have Their Causes, but Consequences Follow ..... 12
Fraud and AML Convergence Today ..... 16
Why Size Does Not Mean Speed ..... 16
Where Convergence Is Happening ..... 17
Does Anyone Own the Convergence Challenge? ..... 21
Technology: Today and Tomorrow ..... 24
Generative and Agentic AI Sit Outside the Rules ..... 25
Technology Is Shared ..... 26
The Outlook: Three to Five Years Out ..... 27
Future Planning ..... 27
Asia-Pacific Is Ahead, and Why ..... 31
Closing the Gap ..... 34
About This Study ..... 35

# List of Figures

Figure 1: U.K. APP Fraud Reimbursement Rate, Before and After Mandatory Rules ..... 8
Figure 2: External Developments Creating Pressure ..... 10
Figure 3: Internal Operational Challenges ..... 11
Figure 4: Obstacles Rated by Significance ..... 13
Figure 5: Consequences of Fraud and AML Operating Separately ..... 15
Figure 6: Fraud and AML Integration Today ..... 16

© 2026 Datos Insights or its affiliates. All rights reserved.

Figure 7: Convergence—Current and Future .....18
Figure 8: Fraud and AML Information Sharing .....20
Figure 9: Who Owns Convergence, by Institution Size .....21
Figure 10: Individual Responsibility for Fraud and AML Strategy.....23
Figure 11: Analytics and AI Capabilities Currently in Use .....24
Figure 12: Institution's Current Ability to Build a Unified Customer Risk View .....25
Figure 13: How Analytics and AI Capabilities Are Deployed Across Fraud and AML ....26
Figure 14: Timeline for Target State Fraud and AML Alignment.....27
Figure 15: Convergence Drivers .....28
Figure 16: Expected Spending Change Over the Next Two to Four Years.....31
Figure 17: Share Targeting Operational Convergence as End State, by Region .....32
Figure 18: Most Significant Obstacle to Alignment, by Region .....33

© 2026 Datos Insights or its affiliates. All rights reserved.

# Summary and Key Insights

Eighty-six percent of financial institutions report missed links between fraud activity and money laundering. That is not a detection failure. It is the predictable output of a structure that puts the fraud signal on one desk and the laundering pattern on another. Fraud teams stop losses in the moment, while AML teams review activity afterward and file on a regulatory clock. Real-time settlement has intensified the gap, and scams and mule networks are precisely where that shows up as a compliance problem rather than a fraud problem alone. A mule account exists to move illicit funds through the banking system and make their origin hard to trace, which is a money laundering function by definition, not just a fraud loss. Once a real-time payment clears into that mule account and clears out again in seconds, with no reversal mechanism, the funds are usually gone before either team has had the opportunity to identify the pattern, flag the account, or file. That is exactly the kind of missed link between fraud activity and money laundering this study is measuring. Institutions have responded by acknowledging the risks associated with a siloed detection and investigation framework, but more is needed.

In a study commissioned by SAS, Datos Insights surveyed 165 fraud and AML executives across seven regions. The aim was not to establish whether institutions believe in working together, but where that belief has produced shared systems, shared staff, and a more dedicated response. Convergence can occur at several levels: technology, data, workflows, governance, and organizational structure. It is best viewed as a continuum rather than a binary state: institutions sit at different points along it, and moving further along does not mean every institution should end at full merger of the two functions.

Key insights from this study include the following:

- **Organizational silos and separate reporting lines are the leading obstacle to alignment, but not the only one that matters.** Eighty-eight percent of institutions rate organizational silos and separate reporting lines as a primary or major barrier, 73% rate technology limitations the same way, and 70% rate data governance and quality issues the same way. These are interconnected barriers, not a single blocker. This separation reflects decades of regulatory and operational divergence. Fraud and AML functions answer to different regulators and run on different legal clocks.
- **Staying separate is not a policy debate. It shows up as missed cases today.** Eighty-six percent of institutions report missed links between fraud activity and money

© 2026 Datos Insights or its affiliates. All rights reserved.

laundering. Model risk management or model governance is currently the most siloed area among respondents, with 39% describing it as largely or fully siloed, ahead of case management workflows, investigation staff, and other areas measured.

- **The tools converge before the teams do, and the gap is now the risk.** Seventy-one percent of institutions say detection technology convergence is already in progress, whereas only 13% say the same for governance and structure. Meanwhile, only 21% of institutions use network analytics and visualization, the case-level analysis that would connect a fraud event to the laundering network behind it. That gap is becoming more significant as payments settle in real time. Investigators have little opportunity to mitigate the loss once they have connected the dots after the fact.
- **Bigger institutions are trying to build something harder.** Large institutions, those above US$500 billion in assets, report the widest obstacle gap compared with smaller peers. Change management resistance, data governance and quality issues, and the absence of a shared workflow or trigger for intelligence exchange are all rated as more significant barriers at this size tier than at small institutions, those under US$100 billion.
- **Asia-Pacific is ahead, and it is not a cultural accident.** Almost seven out of 10 Asia-Pacific institutions are targeting operational convergence, well ahead of other regions. Singapore has a single regulator with authority over both banking and payments, and a legally mandated information-sharing platform, a structural advantage most Western markets do not have.
- **Expected cost savings may be the weakest reason to justify future investments, as it ranks last of the 10 drivers and benefits rated in this study.** Institutions rate improved detection of complex financial crime as the primary driver of future investment, but detection quality is not valued for its own sake. It is rated highly because of what it protects against: 96% of institutions rate regulatory expectations as a primary or major driver, and 89% rate better protection of customers as a primary or major benefit, both far ahead of cost and efficiency pressures.
- **A unified view of the customer remains the exception, not the rule.** Eighty-seven percent of institutions describe their ability to build a unified customer risk view spanning fraud and AML as still partial, with significant gaps remaining. Only 10% call it mostly complete, and 1% call it fully comprehensive.

© 2026 Datos Insights or its affiliates. All rights reserved.

## Staying the Course Will Leave Institutions Behind

The study's findings describe a quantifiable cost of inaction, not a vague warning. An institution that keeps its current pace on governance (meaning case ownership, data-sharing agreements, and shared committee structures) while its peers finish their technology convergence will be the outlier feeling the downside: missed links, duplicate investigations, and higher operating costs. Many institutions, including those with advanced technology convergence, already report those consequences. Technology convergence on its own is not sufficient. It must be paired with the institutional governance and the shared workflows that let teams use the shared technology.

© 2026 Datos Insights or its affiliates. All rights reserved.

# Why the Fraud vs. AML Silo Exists, and Why It Shouldn't Be Retained

It is tempting to treat organizational silos between fraud and AML as a necessary burden, leaving information gaps that shared technologies and dashboards eventually fill. The study says otherwise. Institutions rate organizational silos and separate reporting lines as the leading obstacle to greater alignment, ahead of technology limitations, data governance, and the absence of a shared workflow or trigger for intelligence exchange, though all four are widely rated as significant barriers. The silo is the predictable result of two functions that were built to address different objectives, based upon different regulations, on different legal timelines, and were never designed to be a unified function in the first place.

## Different Mandate, Different Regulators

Fraud prevention exists to stop a loss before it happens or claw it back immediately after. AML compliance is designed to detect and investigate patterns of suspicious activity over time, document them, and report them to a financial intelligence unit within a statutory filing window. The two functions differ in the following ways:

- Fraud answers, in most markets, to a payment or conduct regulator focused on the transaction itself, because fraud carries a direct financial loss for the institution or the customer. In the U.K., the Payment Systems Regulator enforces mandatory reimbursement for authorized push payment (APP) fraud under Specific Direction 20. Unlike fraud, AML compliance is not centered on the same direct financial loss; it is based on customer activity and pattern review of the movement of illicit funds rather than a loss event, which is why it is regulated differently.

- The consequences of getting it wrong also differ sharply: AML failures can result in regulatory fines running into the hundreds of millions or billions of U.S. dollars, and, in the U.S., can jeopardize merger and acquisition approval, while inadequate fraud controls more often result in reputational damage and contested liability disputes with customers. AML compliance functions often answer to a different regulator, the Financial Conduct Authority (FCA) in the U.K. and the Financial Crimes Enforcement Network (FinCEN) in the U.S., though this is not universal. AML operates under statutes and regulations that have no real connection to payment reimbursement. Although regulators have not mandated a convergence of the fraud and AML frameworks across

© 2026 Datos Insights or its affiliates. All rights reserved.

institutions, they have pushed both functions toward increased collaboration and better intelligence sharing.

Technology solutions inherited this split. Organizations built fraud monitoring systems to score transactions in milliseconds and block, allow, or step up authentication before money left the organization. AML detection systems were constructed to run post-transaction in batch, often overnight, scanning completed activity for patterns of unusual or suspicious activity that unfold over days, weeks, or months. These were not two configurations of the same solution. They were often different technologies solving different problems on different timescales. Over the past decade, that split has begun to change. Spurred by the increasing complexity of financial crime, which blurs the once-distinct silos, organizations are looking to bridge the two technology architectures and use systems that support both fraud and AML monitoring, particularly for alert review and case investigation management.

## Real-Time Payments Are Removing the Safety Net

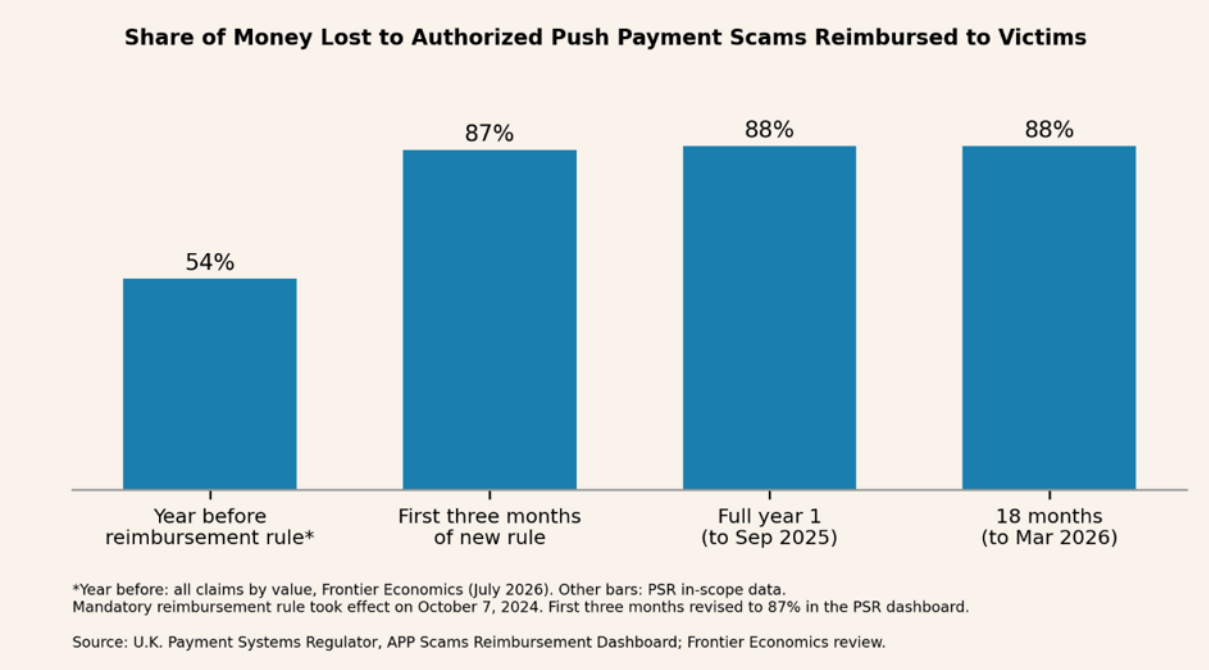
Real-time payment rails are changing the inherent tenets of the historical division. Once a real-time payment settles in seconds across a rail with no reversal mechanism, the money is very often unrecoverable, because the criminal has already moved it through a mule account across borders. Tracing that chain from the original illicit event to the laundering destination is difficult since network analytics and visualization are in use at just 21% of institutions. These techniques are best suited to investigating that chain on a post-settlement basis. This is forensic reconstruction of a loss or a payment tied to an earlier predicate crime, valuable for building a case, but too late to stop the transfer of value. This is becoming a leading argument for increased convergence, and it is a narrower, sharper one than just "fraud and AML should work together." It is that intelligence needs to move between fraud and AML faster than it currently does.

The key integration points are shared data, shared workflows, and shared alert and case management, so that a case can be opened on a converging signal before a payment settles, not stitched together afterward by two teams comparing notes on a case that is already closed. The U.K. regulator's own data shows what happens when a rule forces fraud losses onto the institution's own books rather than the victims' (Figure 1). The Payment Systems Regulator's mandatory reimbursement rule for APP fraud, in force since October 2024, lifted the share of losses returned to victims from 54% before the rule to 65% afterwards, on an all-claims basis, according to an independent review by Frontier Economics. The PSR's own dashboard shows that 88% of in-scope losses were reimbursed over the first 18 months. That is a real shift, and the PSR's evaluation links it to firms

© 2026 Datos Insights or its affiliates. All rights reserved.

reimbursing more victims and investing more in prevention, not only to a change in who bears the loss. It illustrates the kind of lever regulators have available to them: They can shift financial liability and force better outcomes on the fraud side specifically, without ever touching AML supervision, because the two remain separate levers pulled by separate bodies.1

**Figure 1: U.K. APP Fraud Reimbursement Rate, Before and After Mandatory Rules**




## The Battlefield: Intensifying Pressures on All Fronts

Fraud and AML compliance executives identify a plethora of internal and external pressures that are influencing the future strategic and technology investment decisions fraud and financial crime leaders are making or should be making. The internal strains, legacy technology and false positives, call for modernizing what already exists rather than adding a new layer on top of it. The external pressures, AI-enabled fraud and mule networks especially, call for new detection and network-tracing capability. A conversation that only addresses one of these two categories—buying new capabilities while leaving the

[1] "APP scams reimbursement dashboard for Q1 2026," Payment Systems Regulator, updated July 30, 2026 (18 month and first three month figures), and earlier version updated January 30, 2026 (first year figure), accessed October 16, 2026, https://www.psr.org.uk/information-for-consumers/app-scams-reimbursement-dashboard/; Frontier Economics, independent evaluation of the APP scams reimbursement policy, published July 1, 2026, accessed October 16, 2026, https://www.frontier-economics.com/uk/en/news-and-insights/news/news-article-i22383-app-payment-scam-policies-reducing-fraud/.

© 2026 Datos Insights or its affiliates. All rights reserved.

legacy false-positive problem untouched, or modernizing the core platform while leaving mule-network identification and tracing capability absent—is solving only half.

## External Pressures

In November 2024, FinCEN warned U.S. FIs that criminals are using generative AI to create deepfake identity documents, photographs, and videos to circumvent customer identification and due diligence controls.[2] Its published alert sets out red flags for deepfake media, among them customers presenting identity documents that are inconsistent with each other, the use of a third-party webcam plugin during a live verification check, and photos or videos flagged by deepfake detection software. This reinforces what institutions are already seeing. The same fraud patterns institutions rank as top pressures are drawing regulatory attention, confirming the threat is being tracked at the reporting level and not just felt anecdotally on the front line.

AI- or deepfake-enabled fraud and investment and impersonation scams dominate the external pressure ranking, both well ahead of every other category. Sanctions evasion and screening, along with money mule networks, follow as a clear second tier. Crypto or stablecoin financial crime, synthetic identity fraud, and cross-border financial crime sit in a third tier. Trade-based money laundering, first-party fraud, and complex beneficial ownership risk sit at the bottom, each cited by 10% or fewer (Figure 2). These findings reflect general challenges facing the fraud and AML functions individually, rather than convergence-specific findings.

[2] "FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions," Financial Crimes Enforcement Network, November 13, 2024, accessed October 15, 2026, https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf.

© 2026 Datos Insights or its affiliates. All rights reserved.

## Figure 2: External Developments Creating Pressure

**Q. Which external financial crime developments have created the greatest pressure on your institution over the past 12 months? Select up to three.**
(Base: 165 global fraud and AML compliance executives)




Source: Datos Insights survey of 165 fraud and AML compliance executives at global FIs on FRAML convergence, Q3 2026

Ref: 300570

Each of the leading pressures has a specific technology answer:

- AI- or deepfake-enabled fraud calls for identity verification and behavioral biometrics at the point of onboarding or transaction, since this pressure attacks the authentication layer directly, not the detection layer institutions have already built out.
- Money mule networks and sanctions evasion are fundamentally network problems: tracing an account's connections to other accounts, other institutions, and other jurisdictions. Identifying and mitigating mule activity at the point of onboarding or first use is equally important, not only tracing a network once funds have already moved. This is the pressure network analytics and visualization are built to answer, and the clearest link in this survey between a specific external threat and a specific underutilized capability.
- Investment and impersonation scams sit closer to the technology fraud teams utilize, but their proceeds move through the same mule infrastructure AML software is built to

© 2026 Datos Insights or its affiliates. All rights reserved.

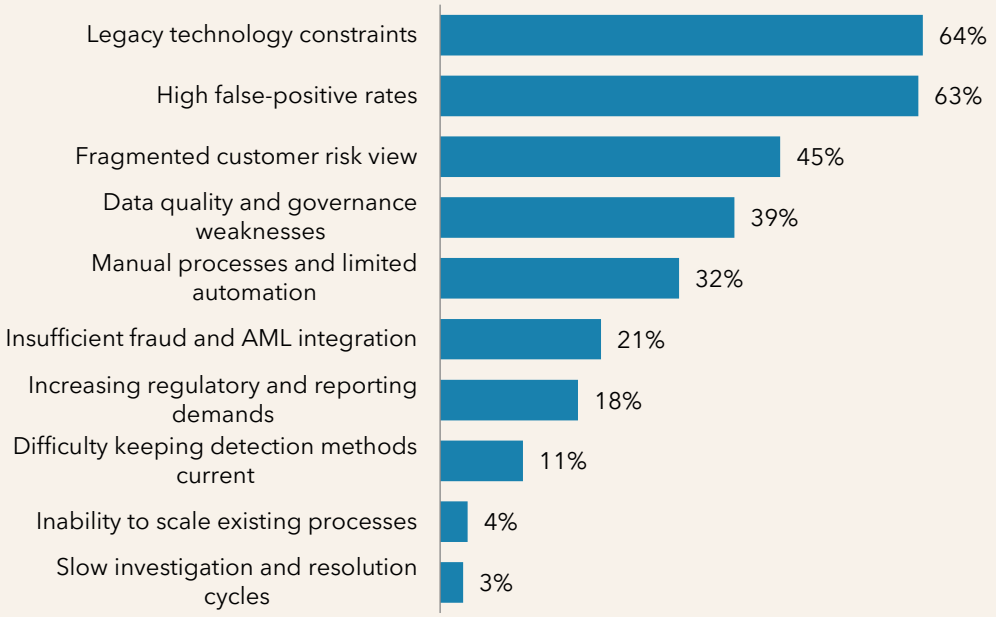
trace, which is precisely the fraud-to-laundering handoff this survey has shown is the weakest link in most institutions' current sharing practices.

## Internal Strain Points to a Technology Refresh Problem

As illustrated in Figure 3, legacy technology constraints and high false-positive rates are the two most cited internal challenges, both well ahead of a fragmented customer risk view and data quality and governance weaknesses. Manual processes and limited automation, along with insufficient fraud and AML integration, follow. Slow investigation and resolution cycles are the least cited internal strain, which is worth noting because it suggests speed of investigation, once a case is opened, is not where institutions feel their operational pain. The pain is earlier: getting the right alert, with the right context, in the first place. As with the external pressures shown in Figure 2, these findings reflect general challenges facing the fraud and AML functions individually, rather than convergence-specific findings.

### Figure 3: Internal Operational Challenges

**Q. Which internal operational challenges place the greatest strain on your institution's fraud and AML functions today? Select up to three.**
(Base: 165 global fraud and AML compliance executives)




Source: Datos Insights survey of 165 fraud and AML compliance executives at global FIs on FRAML convergence, Q3 2026

Ref: 300570

© 2026 Datos Insights or its affiliates. All rights reserved.

## Silos Have Their Causes, but Consequences Follow

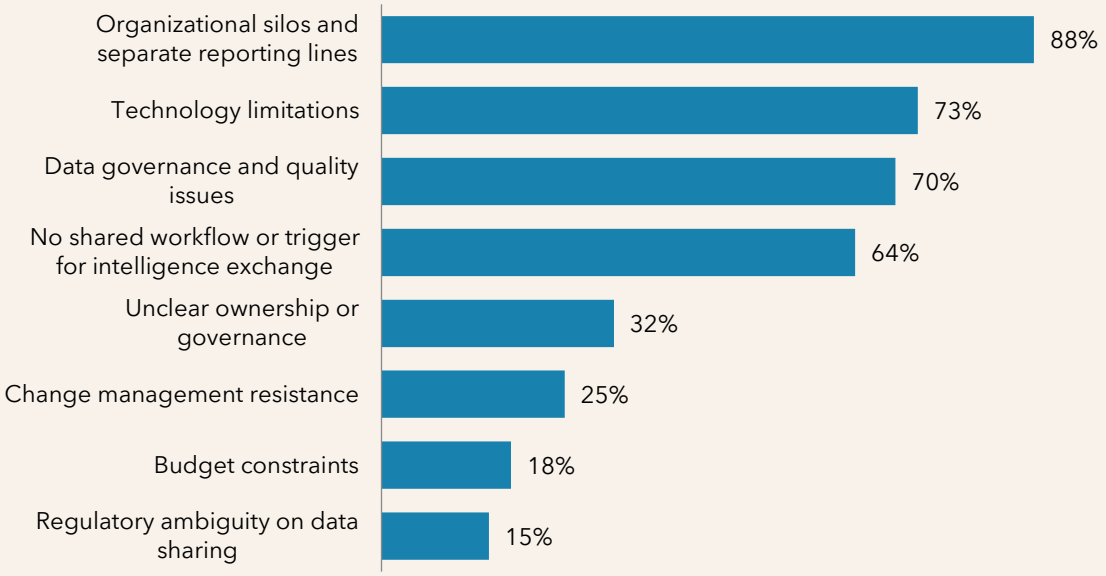
Though fraud and AML were built with separate goals in mind and have genuine structural reasons for existing apart, institutions do not cite these external constraints as their primary obstacle to alignment. Datos Insights believes the technology challenge here is concentrated in legacy, monolithic solutions that have passed their support date and are difficult to manage and update, and in modern solutions that fail to scale across lines of business, not technology in general.

Asking institutions to name their single biggest obstacle may hide the issues inherent in the other obstacles. Fraud and AML compliance executives rated the significance of each obstacle individually (Figure 4).

Organizational silos are identified as a primary or major obstacle by 88% of institutions, ahead of technology limitations (73%) and data governance (70%). Sixty-four percent of institutions separately rate the absence of a shared workflow or trigger for intelligence exchange between fraud and AML as a primary or major obstacle. Closing this gap is frequently a smaller integration project than a platform replacement: connecting two systems that already exist, not replacing either. An institution can leave its reporting lines untouched and still close a meaningful share of the gap by defining and wiring a trigger condition between its fraud and AML systems, a mechanical fix, not an organizational one.

© 2026 Datos Insights or its affiliates. All rights reserved.

### Figure 4: Obstacles Rated by Significance




Source: Datos Insights survey of 165 fraud and AML compliance executives at global FIs on FRAML convergence, Q3 2026

Ref: 300570

Seen this way, the barrier viewpoint is less a single blocker and more of a pyramid that can be built from the bottom up: technology and data first, then organizational structure and governance above them. Once a strong foundation is built, the narrower governance and regulatory questions at the top of the pyramid will increase in importance.

## The Data Protection Constraint

A separate, more solid constraint sits underneath the organizational one. Data protection law does not treat a bank's own retail and corporate divisions as free to share a customer's personally identifiable information with each other, even though that information is key to mitigating risk. Where those divisions are separate legal entities, or separate data controllers within the same group, the U.K. General Data Protection Regulation and equivalent data privacy or protection regimes require a documented legal basis and typically a formal intra-group data-sharing agreement before customer data moves between them, the same rules that apply to two unrelated companies. This maps directly onto the 70% of institutions, as reflected in Figure 4, rating data governance and quality as a major or primary obstacle: A meaningful share of those institutions is very likely a documentation and legal-basis problem, not a purely technical one. In the U.S., Section

© 2026 Datos Insights or its affiliates. All rights reserved.

314(b) of the USA PATRIOT Act provides a voluntary information-sharing safe harbor between institutions, but participation is optional and its practical use remains limited.

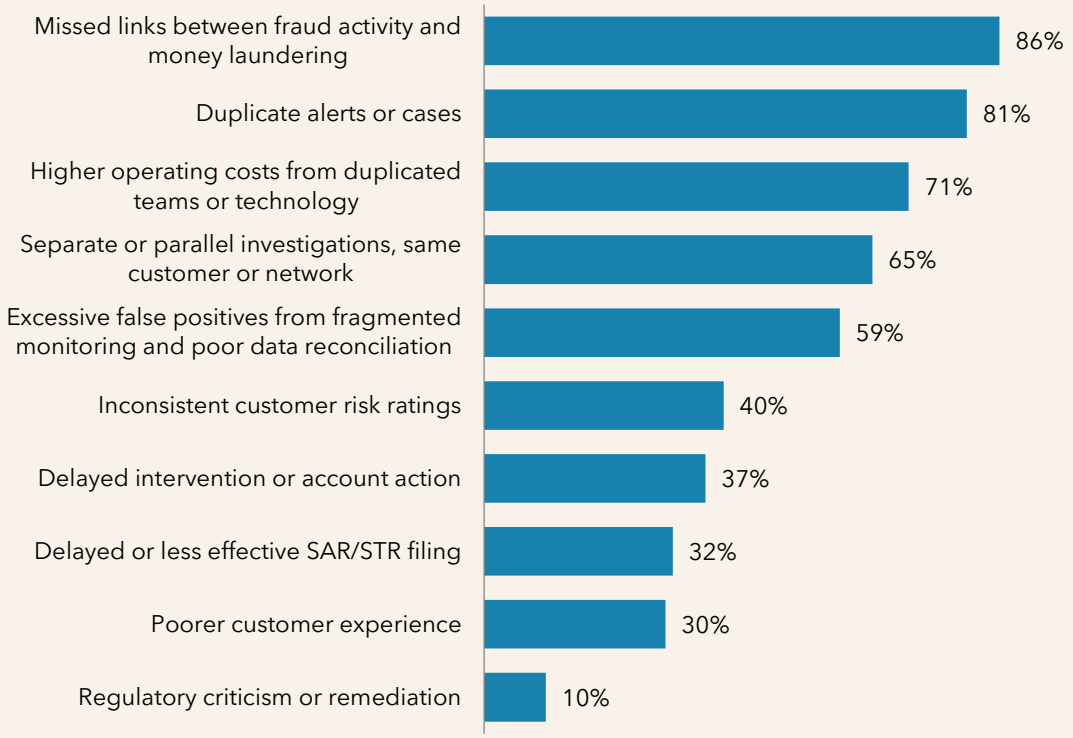
## The Consequences

Every institution is paying a broadly similar price for staying separate. As shown in Figure 5, 86% of institutions report missed links between fraud activity and money laundering as a direct consequence of staying separate, the single most common consequence in the study. Duplicate alerts or cases, higher operating costs, and separate or parallel investigations touching the same customer or network are also cited by roughly two out of every three institutions or more. Together, these consequences describe the cost of not taking advantage of natural integration points between the fraud team and the AML team: shared data, common case management, cross-functional escalation, and shared workflows. They do not make a case for merging the two into a single team or a single detection engine. Duplication of effort, duplication of alerts, and duplication of investigative work on overlapping cases all translate directly.

© 2026 Datos Insights or its affiliates. All rights reserved.

## Figure 5: Consequences of Fraud and AML Operating Separately

**Q. Which consequences has your institution experienced because fraud and AML operate separately or are not fully aligned? Select all that apply.**
(Base: 165 global fraud and AML compliance executives)




Source: Datos Insights Survey of 165 fraud and AML compliance executives at global FIs on FRAML convergence, Q3 2026

Ref: 300570

Thirty-two percent of institutions separately report delayed or less effective suspicious activity filings as a direct consequence of disconnected fraud and AML functions, and 37% report delayed intervention or account action for the same reason. Both figures move together: an institution slow to file is very often also slow to act on the account itself, since the same missing handoff often explains both.

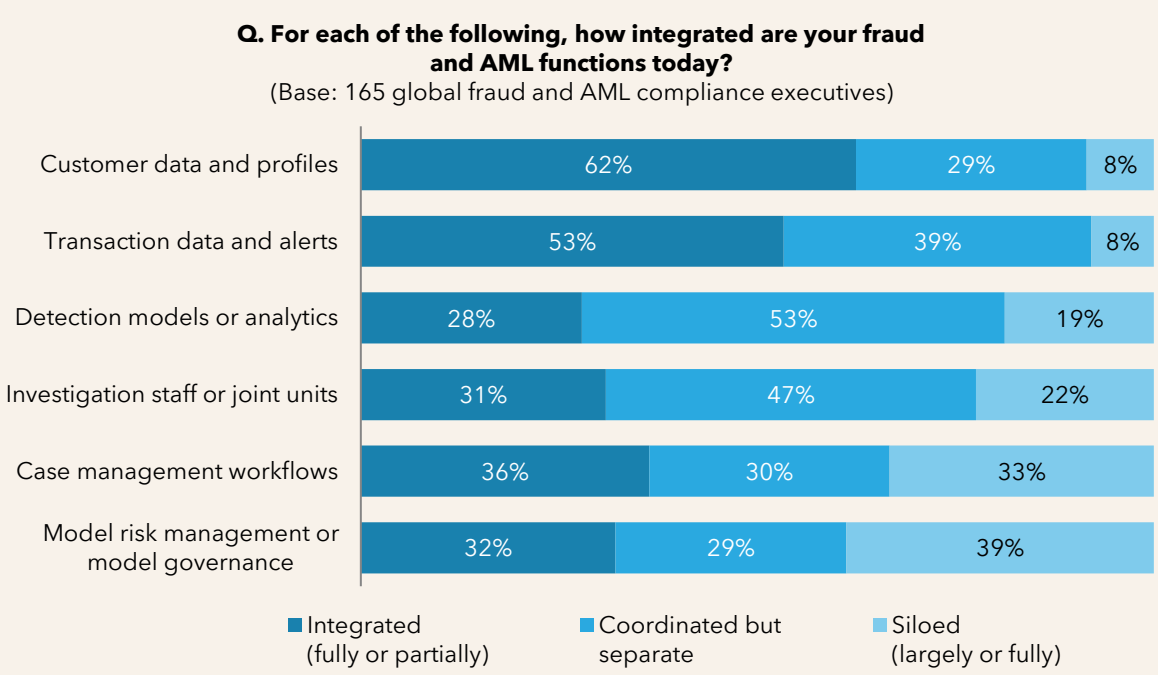
Two further consequences sit lower on the list but still matter: 30% of institutions report a poorer customer experience as a direct result of the separation, and 10% report regulatory criticism or remediation specifically because of it. Both describe a real, currently unmanaged cost sitting downstream of the same handoff problem: a customer flagged twice by two functions, or an institution criticized by a supervisor for exactly the kind of missed link most report experiencing internally.

© 2026 Datos Insights or its affiliates. All rights reserved.

# Fraud and AML Convergence Today

Most institutions have started connecting fraud and AML. The connection is strongest wherever data alone needs to move, and weakest wherever a person, a job title, or a governance process needs to change. This may be because data can move without anyone's job changing. Case management, staff structure, and model governance all require someone to give up ownership, change a reporting line, or accept a different sign-off process, and that is a different, much slower kind of change. As a result, customer data and profiles show the highest reported integration, with case management workflows and investigation staff or joint units sitting further behind (Figure 6). Model risk management is the least integrated area of all, with 39% of institutions calling it largely or fully siloed.

**Figure 6: Fraud and AML Integration Today**




Source: Datos Insights survey of 165 fraud and AML compliance executives at global FIs on FRAML convergence, Q3 2026

Ref: 300570

## Why Size Does Not Mean Speed

It would be easy to assume a large global bank, with a bigger technology budget and the ability to buy or build any technical integration it needs, should converge faster than a smaller regional bank. However, the study does not support that assumption, and the reason is not a lack of technical capability. Two contrasting profiles illustrate why:

© 2026 Datos Insights or its affiliates. All rights reserved.

- A large bank's fraud and AML systems are often spread across multiple business lines, legal entities, and regulatory jurisdictions. Each may have its own operational user interface, risk models, and vendor relationships. Two systems can be integrated technically in weeks, but the harder questions are who owns the shared process, or which of two risk committees signs off on a shared model.
- A regional bank with simpler payments processing, often a single core banking platform for its AML systems, and one investigations team is frequently solving a smaller problem: connecting two systems inside one legal entity, one jurisdiction, one governance structure. The smaller the risk portfolio, the simpler the financial crime detection, so data integration is rarely an obstacle.

For large banks, the obstacle is primarily a governance and legal-entity problem, not a technology one, though legacy, monolithic technology that has passed its support date and requires custom configuration for every change compounds it. No amount of integration middleware resolves who is accountable for the case once the systems are talking to each other.

The larger institution has not solved its silo problem faster. It is working through a different kind of obstacle, because its version of convergence is a larger, more consequential undertaking: a converged operating model across business lines and borders, not a single connected system inside one building, as the preceding discussion of multiple legal entities and risk committees describes.

## Where Convergence Is Happening

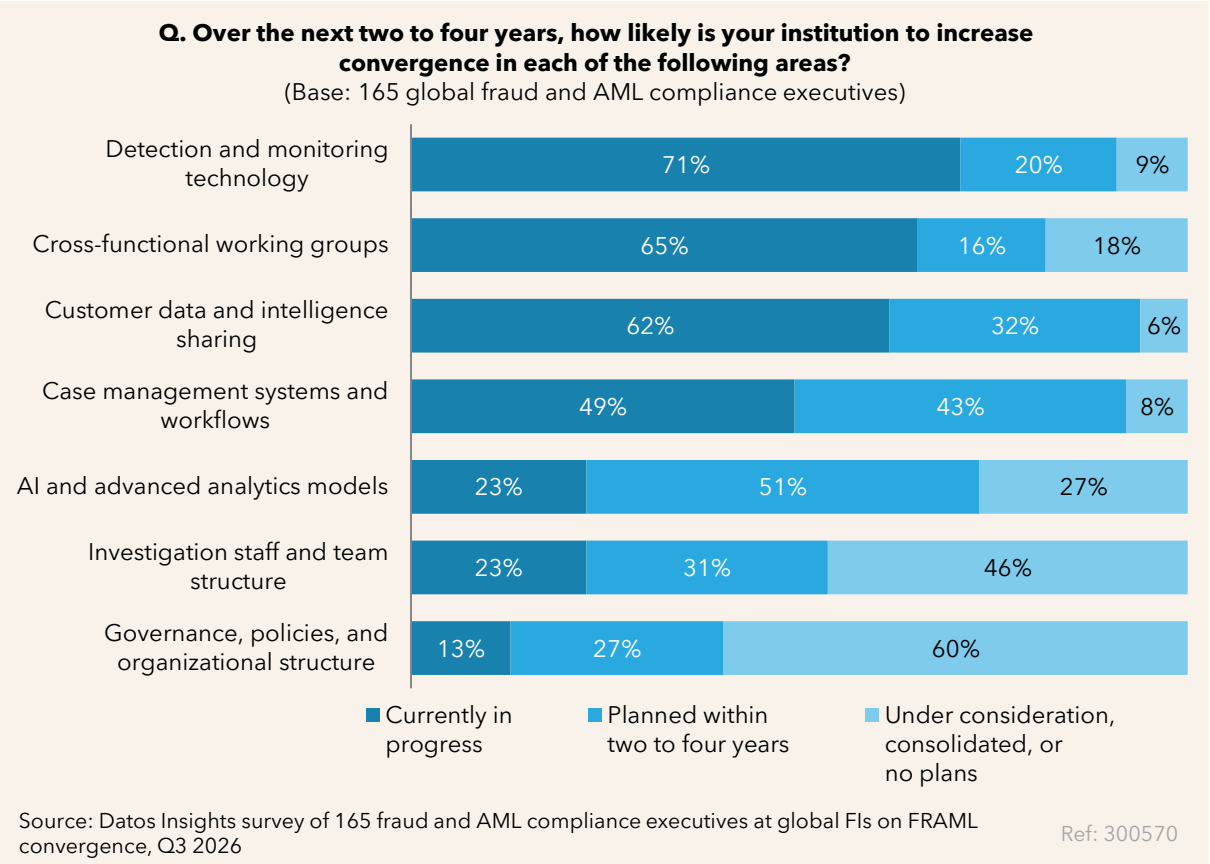
Across all seven areas measured, convergence follows a consistent order, as shown in Figure 7:

- **Detection and monitoring technology leads** (71% currently in progress), followed closely by cross-functional working groups and customer data and intelligence sharing.
- **Case management follows in a middle tier,** while investigation staff structure and AI or analytics models trail at fewer than one out of four institutions each. That middle-tier position reflects current progress only; counting institutions actively converging case management alongside those planning to, it reaches 92%, narrowly ahead of detection and monitoring technology and well ahead of cross-functional working groups (Figure 7).

© 2026 Datos Insights or its affiliates. All rights reserved.

- **Governance, policies, and organizational structure come last** by a wide margin, at just 13% currently in progress, with 60% of institutions still describing them as under consideration or not yet planned.

### Figure 7: Convergence—Current and Future




Source: Datos Insights survey of 165 fraud and AML compliance executives at global FIs on FRAML convergence, Q3 2026

Ref: 300570

Many institutions have not yet converged investigation staff and team structure (Figure 7), which runs against a common assumption that AI reduces the need for people to connect fraud and AML work that still sits in separate teams. Rules-based detection and supervised machine learning dominate adoption, in use at 95% and 90% of institutions (Figure 11), while agentic AI and unsupervised machine learning, the two techniques best placed to act on a pattern without a person framing the rule first, sit at just 5% and 20%, respectively. This gap likely explains why AI is functioning overwhelmingly as a detection and alerting layer rather than a resolution layer: each alert still needs a person to view it in context, connect it to what the other function already knows, and decide what to do. Datos Insights reads that still-manual step as driving an unmet need for a resolution layer rather than only a detection layer, though the survey did not ask respondents to attribute it to a specific cause.

© 2026 Datos Insights or its affiliates. All rights reserved.

Case management and workflow solutions support shared, not merged, ownership. Forty-nine percent of institutions are already converging case management, behind only detection technology, cross-functional working groups, and customer data and intelligence sharing. The demand here is two-part. First, shared signal visibility at the pre-case, alert-investigation stage, seeing that converging fraud, AML, Know Your Customer (KYC), and screening alerts exist on the same party, which itself can be the reason a case gets opened. Second, once a case exists, solutions that let two functions see and work the same case while keeping separate sign-off and compliance ownership, not a single merged queue.

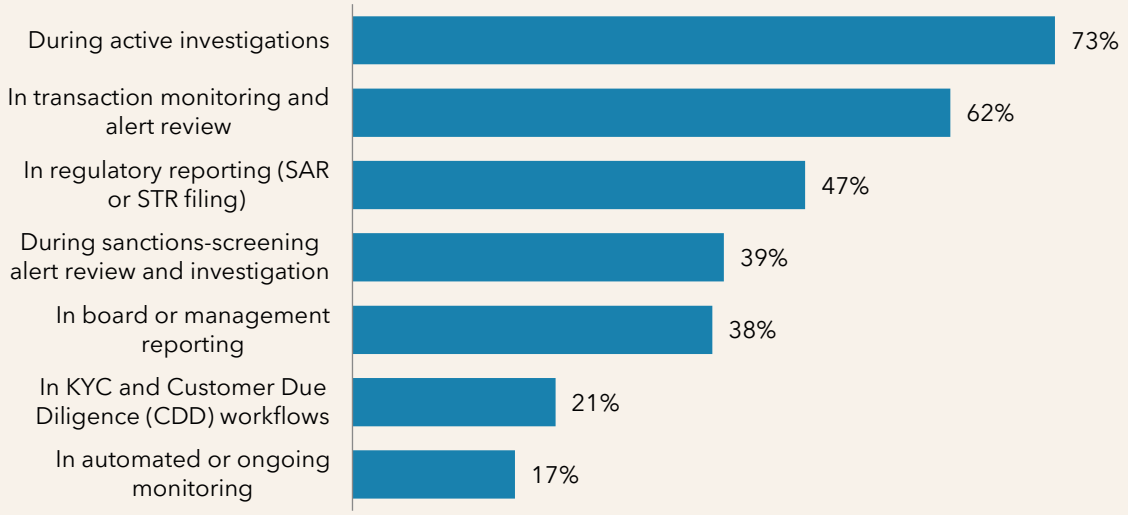
## Information Sharing: Where It Works and Where It Was Never Built

Sharing between fraud and AML is concentrated in one place: the moment a person is already looking at a specific case. Seventy-three percent of institutions share data "often" or "always" during active investigations, and 62% during transaction monitoring and alert review (Figure 8). Sharing falls to 21% for KYC and customer due diligence workflows and to just 17% for automated or ongoing monitoring, the weakest context measured. This distinction matters more than it looks. An institution where an investigator already picks up the phone to a counterpart during a live case can feel, from the inside, as if it has solved cross-domain sharing. But it has only solved the version of sharing that depends on one motivated person deciding to act. The version that runs without anyone needing to notice first, the automated monitoring layer, is almost absent.

© 2026 Datos Insights or its affiliates. All rights reserved.

### Figure 8: Fraud and AML Information Sharing

**Q. How frequently do your institution's fraud and AML teams share intelligence in each of the following contexts? Respondents answering "often" or "always."**
(Base: 165 global fraud and AML compliance executives)




Source: Datos Insights survey of 165 fraud and AML compliance executives at global FIs on FRAML convergence, Q3 2026

Ref: 300570

## Closing the Gap Is a Workflow Task

This points to a specific and addressable priority, not a vague call for more collaboration. Institutions do not need to invent cross-domain sharing from nothing. The case-level version already works and works well. What is missing is moving that same intelligence-sharing logic into the automated, systemic layer, the layer that runs without a person deciding to act, because that is the only layer fast enough to matter once settlement happens in seconds rather than days. Practically, this is a workflow and integration task (defining what event on the fraud side should automatically generate a flag on the AML side and vice versa) not a reorganization. It is the kind of task a dedicated process owner, the role this report's obstacle data points to as largely missing, would be built to run.

This pattern is visible not only in this study's data. The U.K.'s FCA promotes a partnership approach to tackling fraud and encourages collaboration across regulated firms and other fraud partners. This study's findings point to the same need for shared intelligence.[3]

[3] "Fraud," Financial Conduct Authority, accessed October 15, 2026, https://www.fca.org.uk/firms/fraud.

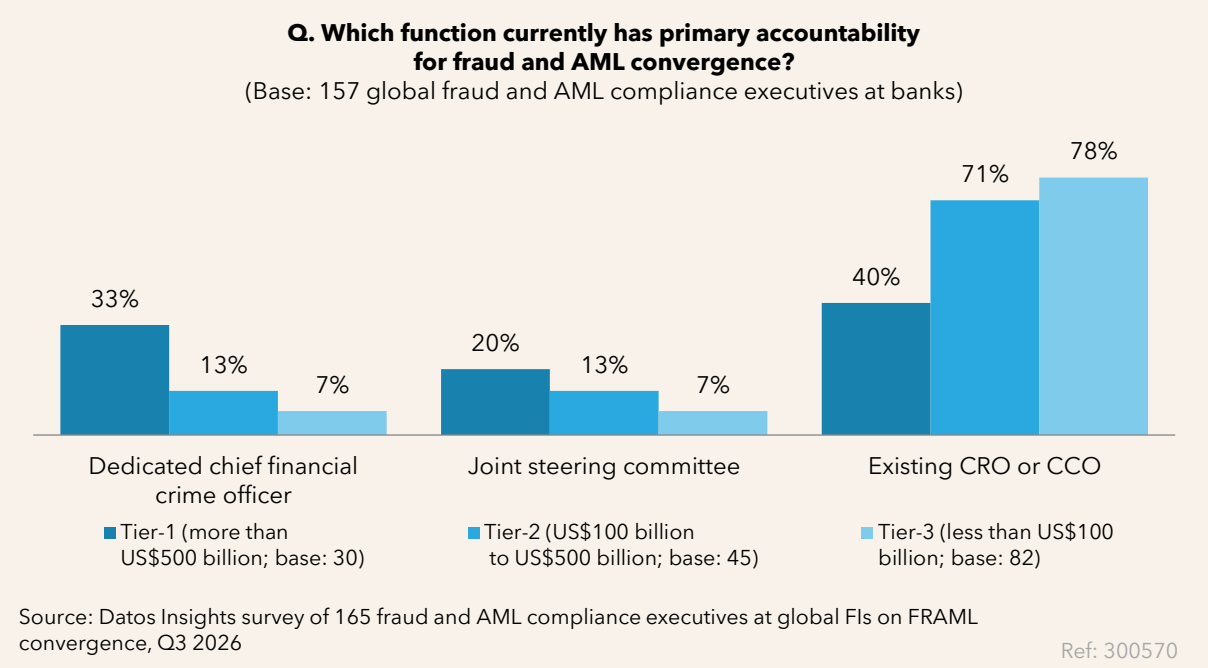
© 2026 Datos Insights or its affiliates. All rights reserved.

# Does Anyone Own the Convergence Challenge?

At most institutions, AML compliance is overseen by either the chief compliance officer or the chief risk officer, with a small segment through a dedicated chief financial crime officer. The fraud team typically sits inside the business or under a chief risk officer. This is noteworthy. An AML compliance leader's incentives—audit readiness, regulatory defensibility, and documented processes—are not automatically the same as a fraud leader's incentives of speed and loss prevention. Any internal case for convergence should be built for both audiences.

Where convergence has an owner, that owner is most often the chief risk officer or the chief compliance officer, with some institutions having established a dedicated chief financial crime officer role and a joint steering committee. As demonstrated in Figure 9, sharp differences exist by size. Among large institutions, 33% have a dedicated chief financial crime officer role and a further 20% run a joint steering committee. Among small institutions, 7% have each, and 78% still run convergence through an existing chief risk officer or chief compliance officer, for whom it is one responsibility among many rather than a dedicated mandate.

### Figure 9: Who Owns Convergence, by Institution Size




Source: Datos Insights survey of 165 fraud and AML compliance executives at global FIs on FRAML convergence, Q3 2026

Ref: 300570

© 2026 Datos Insights or its affiliates. All rights reserved.

## Dual Ownership Rises With Institution Size

Dual or shared ownership—a dedicated chief financial crime officer or a joint steering committee—rises steadily with institution size: 14% of small institutions report it, against 26% of midtier and 53% of large institutions (Figure 9). Larger institutions have deliberately created senior roles that own both functions, matching the higher share of dedicated chief financial crime officer roles. Smaller institutions rely far more on a single risk or compliance leader covering both areas informally, which this report captures in its figures on existing chief risk officer and chief compliance officer ownership rather than as dual responsibility. Midtier institutions sit between the two: large enough to have separated the roles but slower to formalize joint ownership over them than the largest institutions.

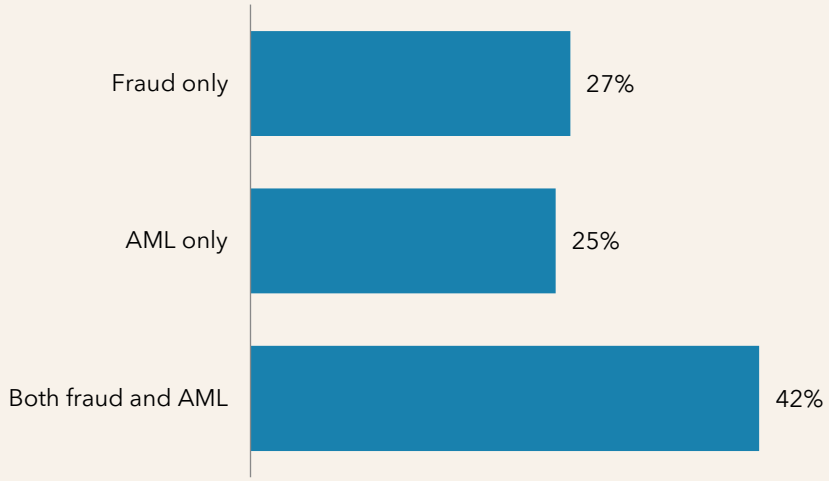
## Individual Accountability Beyond the Organizational Chart

Convergence is often thought of as something institutions build at the structural level: new committees, shared systems, and redrawn reporting lines. The study also examined who holds personal responsibility for convergence outside the organizational construct, and the findings tell a different story. Forty-two percent of surveyed respondents describe themselves as responsible, not merely a contributor, for both fraud detection strategy and AML compliance strategy. A further 27% are responsible for fraud alone and 25% for AML alone (Figure 10). In other words, in more than four out of 10 cases in this survey, one person is already doing the job this entire report has described institutions struggling to build a structure for.

© 2026 Datos Insights or its affiliates. All rights reserved.

## Figure 10: Individual Responsibility for Fraud and AML Strategy

**Q. In your current role, are you responsible for any of the following?**
(Base: 165 global fraud and AML compliance executives)




Source: Datos Insights survey of 165 fraud and AML compliance executives at global FIs on FRAML convergence, Q3 2026

Ref: 300570

For many institutions, creating a new dedicated integration role is not the inherent challenge, because a senior leader already effectively holds both halves of the job informally. The practical task may be formally recognizing and resourcing that person, giving the individual a real title, a real budget line, and real authority over strategic and technology investment decisions, rather than leaving the connection between fraud and AML dependent on one individual's informal reach across two job descriptions. Of the 70 surveyed respondents personally responsible for both fraud and AML strategy, only 42% are responsible for financial crime technology or vendor selection, and only 34% are responsible for financial crime budgets or investment decisions. The individual most likely to want a converged solution, because that person sees both sides of the problem, is not the person who owns the decision or the funding to buy it.

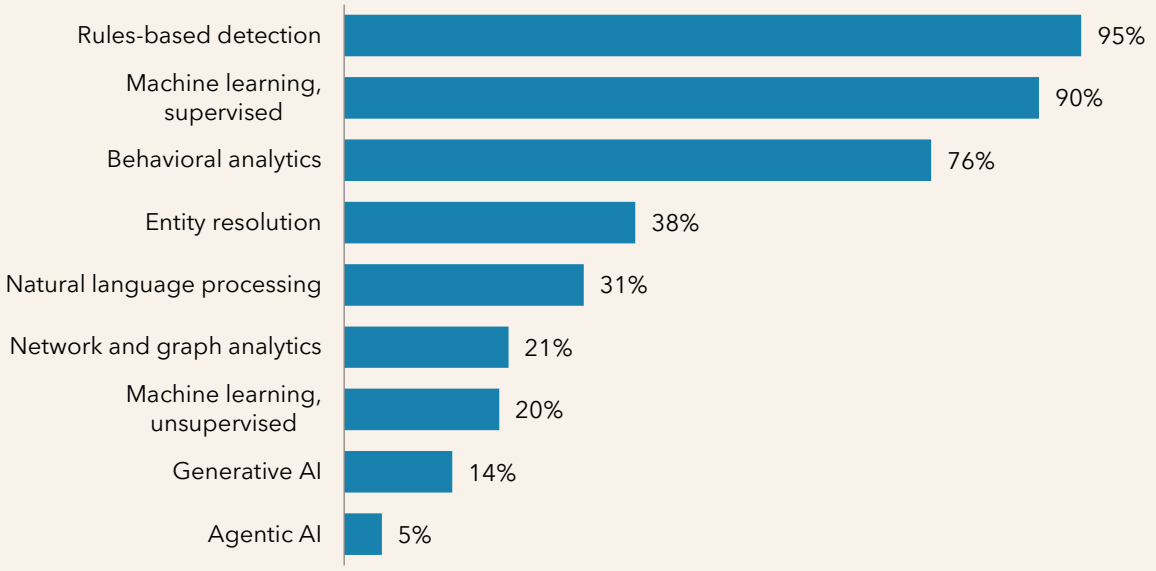
© 2026 Datos Insights or its affiliates. All rights reserved.

# Technology: Today and Tomorrow

Rules-based detection and supervised machine learning are in use almost everywhere, with behavioral analytics having similar ubiquity (Figure 11). From there, adoption falls off quickly as entity resolution, natural language processing, network analytics and visualization, and unsupervised machine learning are in use at less than 40% of institutions each. Generative AI is in use at 14% of institutions, well behind those established techniques but still meaningfully ahead of agentic AI, the newest category, at just 5%. Agentic AI remains the single capability furthest from mainstream adoption, which is consistent with the explainability standard supervisors apply to any model driving a customer or financial crime decision, since a rules-based or supervised system is much easier to document and defend to regulators than a generative or agentic one.

### Figure 11: Analytics and AI Capabilities Currently in Use

**Q. Which of the following analytics and AI capabilities does your institution use today?**
(Base: 165 global fraud and AML compliance executives)




Source: Datos Insights survey of 165 fraud and AML compliance executives at global FIs on FRAML convergence, Q3 2026

Ref: 300570

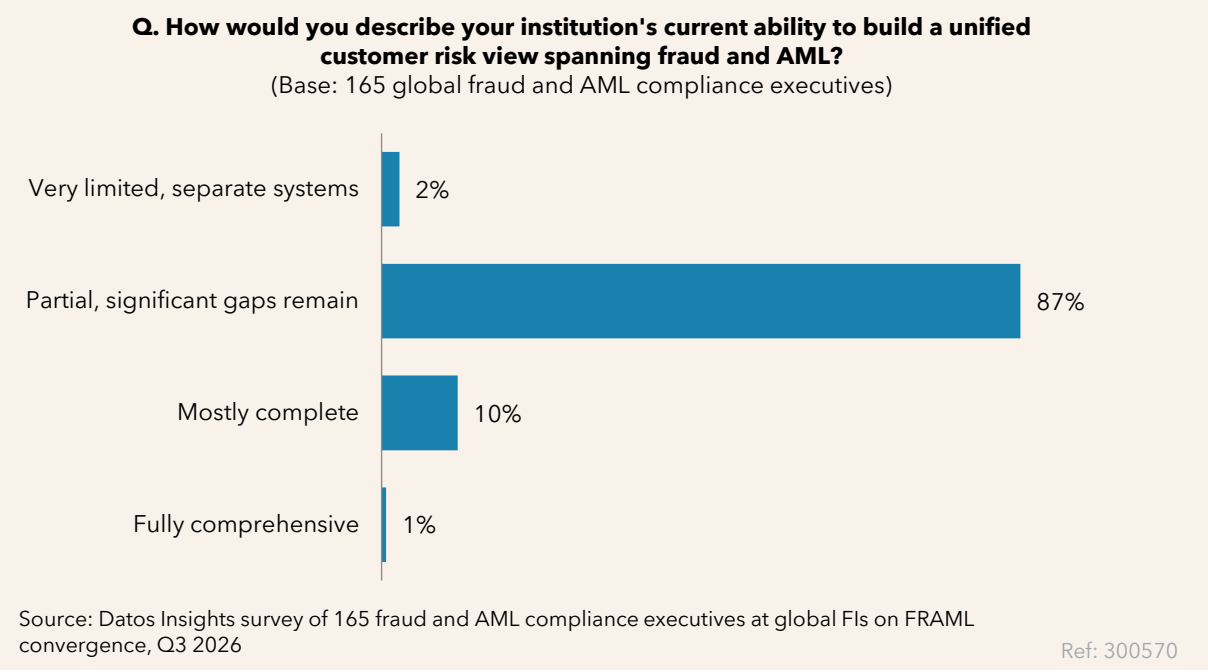
It would be easy to assume network analytics and visualization are new and unproven. They are not; these techniques have existed in fraud and AML tooling for years. The slower adoption may reflect a more fundamental challenge: network analytics and visualization only produce value once an institution has already solved a harder problem this report has described throughout—a single, connected view of customers and their transactions across

© 2026 Datos Insights or its affiliates. All rights reserved.

fraud and AML. Eighty-seven percent of institutions describe their ability to build that unified customer risk view as still partial, with significant gaps remaining (Figure 12).

Network analytics and visualization that run on a fragmented, siloed data foundation surface fragmented, siloed results. The technology gap here is downstream of the organizational gap this report opened with, not a separate problem.

**Figure 12: Institution's Current Ability to Build a Unified Customer Risk View**




Source: Datos Insights survey of 165 fraud and AML compliance executives at global FIs on FRAML convergence, Q3 2026

Ref: 300570

## Generative and Agentic AI Sit Outside the Rules

There may be a separate, more concrete reason for the lag of generative and agentic AI. A rules-based system sits inside an explainability framework that banks and their examiners already know how to apply. Generative and agentic AI currently do not, though generative AI's head start suggests institutions are finding more immediate, lower-risk applications for it, likely in drafting and summarization tasks adjacent to the decision itself, rather than in the decision-making step that draws direct supervisory scrutiny. Agentic AI, which by design takes independent action rather than assisting a human decision-maker, faces that scrutiny most directly, which is a specific, sourced reason it remains the single capability furthest from mainstream adoption.

For example, in April 2026, the Office of the Comptroller of the Currency, the Federal Reserve, and the Federal Deposit Insurance Corporation jointly issued revised interagency

© 2026 Datos Insights or its affiliates. All rights reserved.

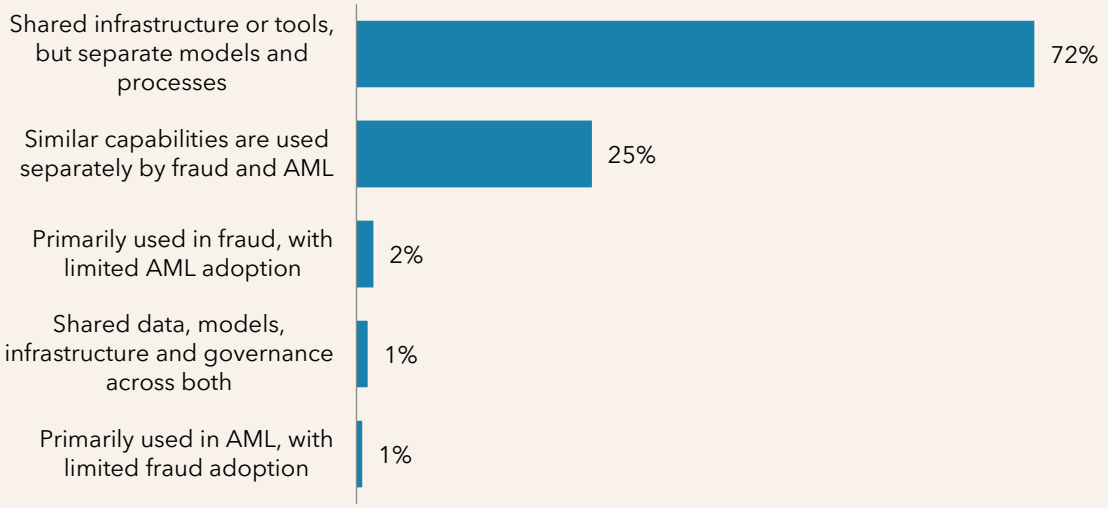
model risk management guidance, replacing the framework banks had followed since 2011, and stated explicitly that generative AI and agentic AI models are novel and rapidly evolving and are outside the scope of that guidance.[4] In practice, that leaves an institution deploying either technology in a fraud or AML context without a settled supervisory framework to validate it against.

## Technology Is Shared

Seventy-two percent of institutions describe their analytics and AI capabilities as running on shared infrastructure but with separate models and processes for fraud and AML (Figure 13). Only 1% run fully shared data, models, infrastructure, and governance across both. This illustrates that the part of convergence that is most cost-effective to build, a shared platform, has gone furthest. The mechanisms that require the two functions to trust and use the same model remain rare.

### Figure 13: How Analytics and AI Capabilities Are Deployed Across Fraud and AML

**Q. Which statement best describes how your institution's advanced analytics and AI capabilities are deployed across fraud and AML?**
(Base: 165 global fraud and AML compliance executives)




Source: Datos Insights survey of 165 fraud and AML compliance executives at global FIs on FRAML convergence, Q3 2026

Ref: 300570

[4] "Model Risk Management: Revised Guidance," Office of the Comptroller of the Currency, April 17, 2026, accessed October 15, 2026, https://www.occ.gov/news-issuances/bulletins/2026/bulletin-2026-13.html.

© 2026 Datos Insights or its affiliates. All rights reserved.

# The Outlook: Three to Five Years Out

Technology and data convergence are already well underway. Detection technology, cross-functional working groups, and intelligence sharing will largely be complete within this window. Most institutions expect to reach their target state within three to five years, and an occasional organization envisions a target state within 12 months (Figure 14). Governance and internal organizational structure will not move at the same pace. Absent a strategic realignment, institutions on their current trajectory will enter the next window with a converged technology stack sitting atop an unconverged governance structure.

**Figure 14: Timeline for Target State Fraud and AML Alignment**




Source: Datos Insights survey of 165 fraud and AML compliance executives at global FIs on FRAML convergence, Q3 2026

Ref: 300570

Every institution planning its next three to five years must make several key decisions as it advances its fraud and AML frameworks and how they bring those two functions closer together: which use cases and underlying technologies to prioritize, whether to reengineer its organizational structure, and which internal role should own convergence.

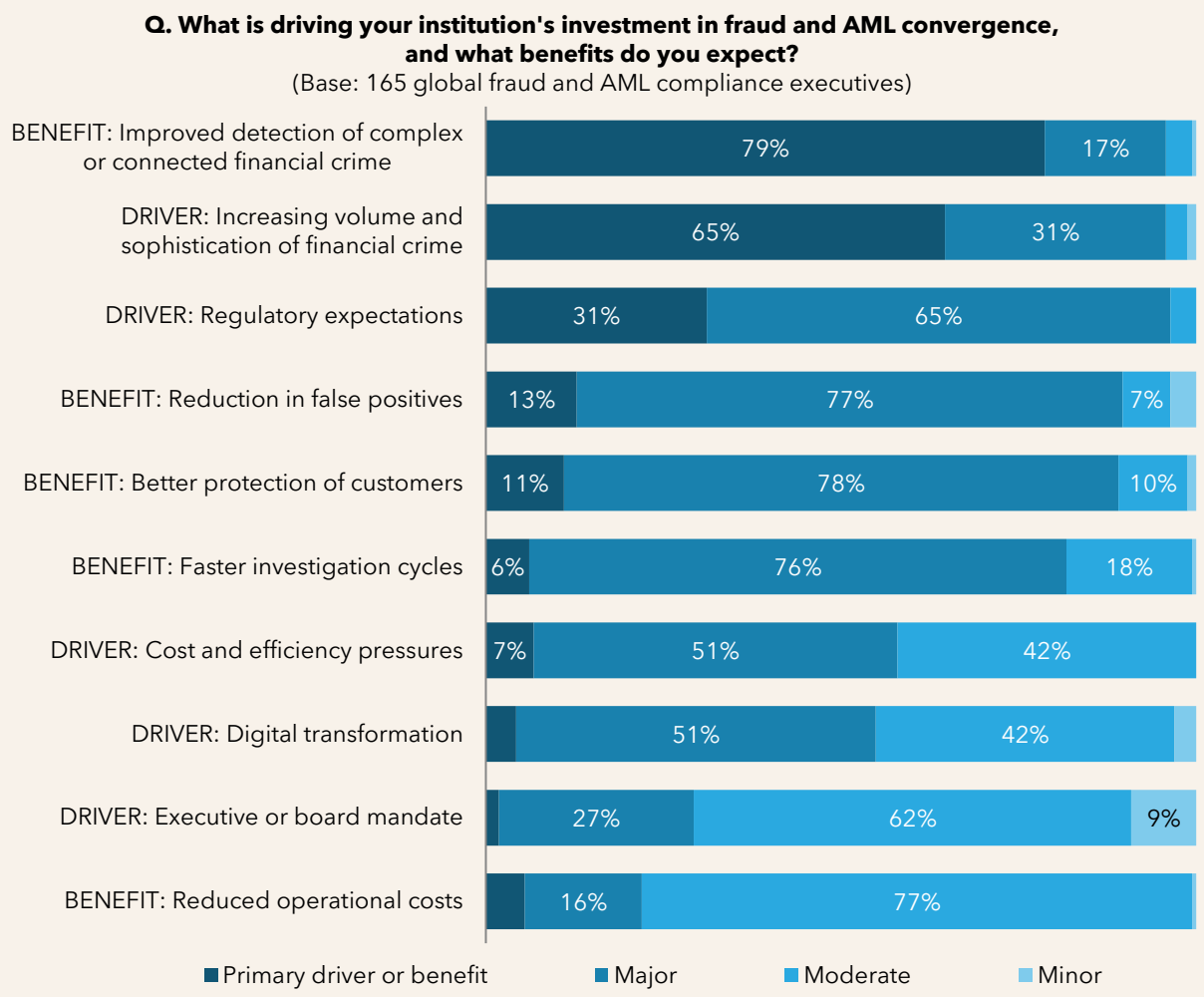
## Future Planning

Rather than asking institutions to pick a single reason for investing, the study asked respondents to rate the significance of specific drivers and benefits. As shown in Figure 15,

© 2026 Datos Insights or its affiliates. All rights reserved.

improved detection of complex or connected financial crime is rated as the primary reason, with increasing volume and sophistication of financial crime and regulatory expectations as other strong drivers. This reflects what each new strategic investment should lead with: detection quality against a rising, complex threat, not cost, not a board mandate, not a compliance deadline.

### Figure 15: Convergence Drivers




Source: Datos Insights survey of 165 fraud and AML compliance executives at global FIs on FRAML convergence, Q3 2026

Ref: 300570

Every one of the 10 is rated major or primary by more than half of institutions except two: executive or board mandate and reduced operational costs (both at less than 30%). That is a useful finding: cost reduction is a weak justification for convergence spend. It is close to the weakest one measured, ranking below every driver related to detection quality,

© 2026 Datos Insights or its affiliates. All rights reserved.

customer protection, or investigation speed. An institution, or a vendor, building a business case primarily around cost savings is often arguing from the weakest point.

Often convergence requires a carefully choreographed sequence of multiple interdependent steps. A shared case management system needs the underlying data and technology connected first. A change to investigation staff structure or reporting lines needs somewhere for those staff to work once the change happens. Governance and organizational structure changes—new reporting lines, a new accountable executive, a redrawn committee structure—sit at the end because they are the most expensive to reverse if the underlying technology and process foundation is not yet solid. Institutions are, in effect, de-risking the hardest and most disruptive part of convergence by doing it last, after the parts that can be tested and adjusted without touching a single person's job.

The risk in this approach is not that it is wrong. It is that it can quietly become permanent. An institution that has converged its technology, its data, and its working groups has completed the parts of convergence that deliver visible, low-risk wins. Governance and structure, the part this report's obstacle data identifies as a major component of the convergence problem, is also the part with the least momentum behind it. Nothing in the sequence forces an institution to complete the final stage. Left alone, "planned within two to four years" can become the answer indefinitely.

## Building the Internal Team

The clearest staffing gap is not headcount, but rather which role owns convergence. Organizational silos, the top-rated obstacle, require a governance decision only leadership can make. As noted, few institutions have a dedicated chief financial crime officer or equivalent or run a joint fraud-AML steering committee. This absence of ownership has real consequences: institutions continue to run duplicated teams and technology, pursue separate or parallel investigations touching the same customer or network, and incur higher operating costs as a result. The gap is not theoretical; it manifests directly in the operational inefficiencies institutions are already reporting today.

Yet solving this gap does not require an institution to overhaul its entire structure. Weighed against the consequences of continued separation, a single strategic hire (a dedicated chief financial crime officer or equivalent) or a formal joint steering committee with real budget authority is a comparatively small investment. Many institutions already have someone informally doing this work, connecting fraud and AML across organizational boundaries through individual reach and informal influence. The practical task may be formalizing that role, resourcing it to match the responsibility.

© 2026 Datos Insights or its affiliates. All rights reserved.

## Practical Steps Short of a Governance Overhaul

Not every institution can, or should, wait for a full governance restructuring before getting real value from convergence. Technology and case-level moves, such as network analytics and visualization, a shared trigger layer, and formalizing case-level sharing, are the fastest available levers. There is also an external clock worth factoring into that timing, separate from anything institutions control internally.

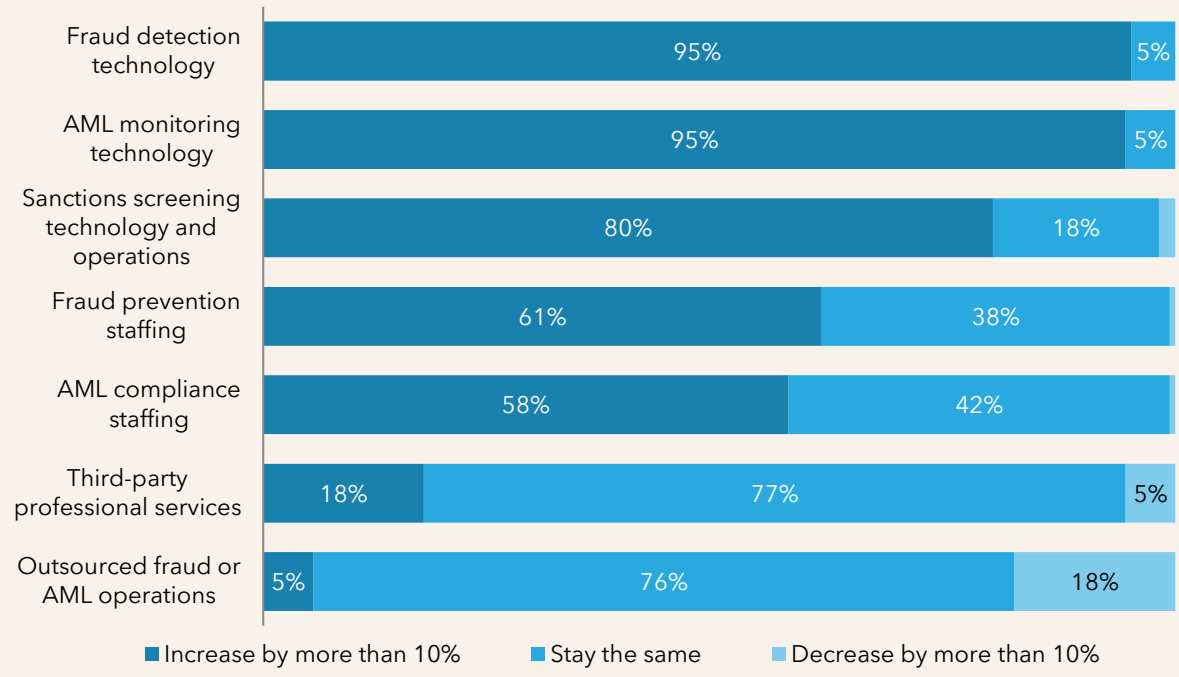
For institutions operating in the EU, the Anti-Money Laundering Regulation applies directly across all member states in July 2027, replacing the current patchwork of national AML laws with a single rulebook, and the Anti-Money Laundering Authority is expected to begin selecting the first institutions for direct supervision shortly after. The practical detail worth noting is not just the date but the shift in what supervisors are asking to see: increasingly, whether a control produces a demonstrable, measurable outcome, not whether a policy document describing it exists. A governance structure that looks adequate on paper—a committee charter, a policy binder—is not the same evidence a supervisor working to that standard will accept. Institutions with a 2027 compliance deadline already on their calendar may find that the case-level and technology investments available now double as early, visible progress toward that separate requirement, rather than treating the two as unrelated projects competing for the same budget.

## Outsourcing: A Good Idea?

Outsourced fraud or AML operations spend is one category where more institutions plan to cut than grow, as 18% expect a decrease against just 5% expecting an increase (Figure 16). Read together with the staffing increases in Figure 16 (61% expect spending on fraud prevention staffing to rise by more than 10%, and 58% expect the same for AML compliance staffing), institutions appear to be treating convergence-specific judgment work, connecting a fraud signal to a laundering pattern using knowledge of a specific customer or institution, as something to build and keep in-house rather than something to buy as a managed service. Institutions weighing this choice may find it useful to distinguish between the technology and workflow layer, which may be reasonable to source externally, and the judgment work itself, which institutions are increasingly choosing to keep in-house.

© 2026 Datos Insights or its affiliates. All rights reserved.

### Figure 16: Expected Spending Change Over the Next Two to Four Years




Source: Datos Insights survey of 165 fraud and AML compliance executives at global FIs on FRAML convergence, Q3 2026

Ref: 300570

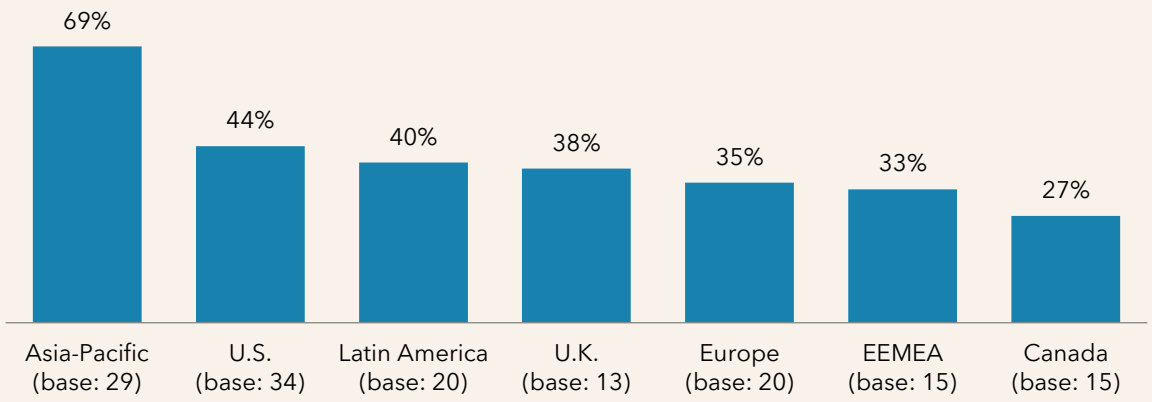
## Asia-Pacific Is Ahead, and Why

Asia-Pacific institutions, including those in Singapore, report the highest rate of targeting operational convergence as their end state, at 69%, well ahead of the U.S. and Canada (Figure 17). Singapore may help explain this result: the MAS is one regulator with authority over both banking supervision and payments, rather than the split that exists in the U.S. and the U.K.

© 2026 Datos Insights or its affiliates. All rights reserved.

### Figure 17: Share Targeting Operational Convergence as End State, by Region

**Q. What is your institution's target state for the relationship between fraud and AML? Respondent answering "operational convergence."**
(Base: 146 global fraud and AML compliance executives*)




*the question was reworded partway through fielding, resulting in a smaller sample size compared to the rest of the survey

Source: Datos Insights survey of 165 fraud and AML compliance executives at global FIs on FRAML convergence, Q3 2026

Ref: 300570

Under its authority, MAS established the Collaborative Sharing of ML/TF Information & Cases (COSMIC), a legally mandated platform that enables Singapore banks to share financial crime intelligence with each other directly. This does not mean Singaporean banks are inherently better at internal convergence than U.S. or European banks. It means Singapore's regulatory structure creates fewer barriers to this kind of collaboration than structures in the U.S. and Europe, where responsibilities are more divided.

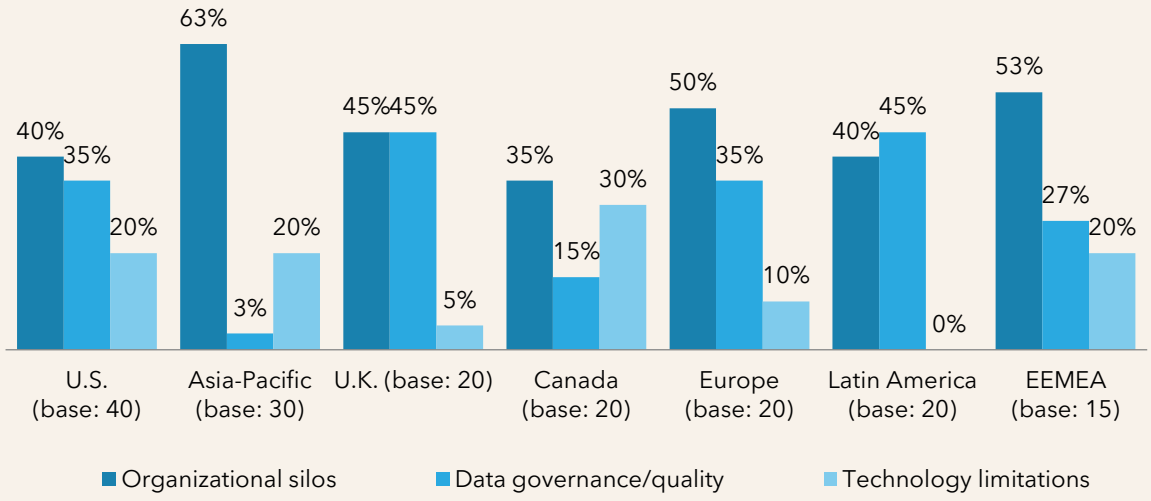
## The Obstacle by Region

Figure 18Asked separately to name the most significant barrier to greater alignment, respondents in five of the seven regions chose organizational silos, from 35% in Canada to 63% in Asia-Pacific (Figure 18). Latin America breaks this pattern, with data governance and quality issues leading at 45%, ahead of organizational silos at 40%. In the U.K., the two are tied at 45% each. This is worth regarding carefully rather than dismissing as noise. In markets where the organizational groundwork for convergence is comparatively advanced, the visible obstacle shifts to the data layer itself: cleaning, matching, and reconciling the underlying customer and transaction records well enough to make a converged view worth having.

© 2026 Datos Insights or its affiliates. All rights reserved.

## Figure 18: Most Significant Obstacle to Alignment, by Region

**Q. Which of the following is the most significant barrier to greater alignment between fraud and AML?**
(Base: 165 global fraud and AML compliance executives)




Source: Datos Insights survey of 165 fraud and AML compliance executives at global FIs on FRAML convergence, Q3 2026

Ref: 300570

The Asia-Pacific's especially concentrated silo obstacle, at 63% against just 3% citing data governance, suggests the opposite: an environment where the organizational work is still the dominant task, even where the regulatory groundwork is comparatively favorable.

In the five regions where they lead, organizational silos remain the dominant, unresolved obstacle, and an internal business case built around structure and ownership, not data cleanup, will match what institutions in those regions are reporting.

© 2026 Datos Insights or its affiliates. All rights reserved.

# Closing the Gap

Fraud and AML working as one connected view inside a single institution is not a rebrand of an old idea. It is a response to payment systems that now move money faster than the two functions built to police it were designed to react. The disconnect between fraud and AML was a defensible design choice when there was time to investigate after the fact. Real-time settlement has quietly removed that time. Technology and data convergence are already well underway and delivering value. Organizational and governance convergence, the part that would let a fraud signal and a laundering pattern be reviewed together, through shared workflows, rather than in separate silos, is lagging.

Five recommendations follow for fraud and AML leaders as they look into the future and build better defenses against a common enemy. These are principles institutions can apply according to their own target operating model and maturity, not a single prescribed path; the appropriate structure and investment sequence may differ by institution. The recommendations are as follows:

- **Establish an owner accountable for a bridge between fraud and AML.** This should be someone whose job is to define, build, and maintain the automatic handoffs between fraud and AML and the underlying teams and systems.
- **Base the internal business case on detection quality** rather than cost, as it may carry more weight in this environment. Reduced operational cost ranks last of the 10 drivers and benefits rated in this study; improved detection of complex financial crime ranks first by a wide margin.
- **Choose strategic partners in this journey based upon expanded expertise and solution portability and signal strength.** Treat signal ownership and model portability as selection criteria, but keep the judgment work in-house. Institutions cutting outsourced fraud and AML operations outnumber those growing them.
- **Explore network analytics and visualization for earlier investment**, because it is the capability most directly tied to the top-rated investment driver, improved detection of complex financial crime, and pair it with unified customer view work, since its value depends on that foundation.
- **Address the intra-group data-sharing question.** It will be easier to resolve as a documented legal and governance exercise ahead of time, rather than leaving it to surface as a blocker during a larger reorganization.

© 2026 Datos Insights or its affiliates. All rights reserved.

# About This Study

This report was commissioned by SAS and is based on a survey of 165 fraud and AML compliance executives across 21 countries and seven regions, spanning commercial banks, retail banks, corporate and investment banks, and fintech firms. Respondents hold direct responsibility for fraud detection, AML compliance strategy, financial crime technology selection, or financial crime budgets, and were screened for current employment and genuine seniority in the field. Institution size is reported using three tiers defined by total assets: Small institutions hold less than US$100 billion, midtier institutions hold between US$100 billion and US$500 billion, and large institutions hold more than US$500 billion. Fintech firms are screened separately by annual revenue. The survey was conducted online between July 8 and August 21, 2026, with respondents recruited through Datos Insights' own professional networks and third-party recruitment partners. The survey covered current cross-domain challenges and priorities, current and planned convergence strategies, shared technologies and data, and appetite for new solutions, capabilities, and investment. The data for the survey has a margin of error of 7 points at the 90% level of confidence; statistical tests of significance between segments were conducted at the 90% level of confidence.

© 2026 Datos Insights or its affiliates. All rights reserved.

For more information, please visit sas.com/framl.



SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration.
Other brand and product names are trademarks of their respective companies. Copyright © 2026, SAS Institute Inc. All rights reserved. W1721100.1026