NICE Actimize

Regulation Asia

Report

AML Tech Barometer 2026

Convergence, Crisis, and Control: The New Financial Crime Equation

Contents

1. Executive Summary 3
2. Introduction 6
3. About the 2026 AML Tech Barometer 7
4. Methodology 8
5. The Evolving Threat Landscape 9
6. Q&A with Sungyong Kang, INTERPOL 13
7. Financial Crime and Technology Priorities 15
8. Q&A with Milan Gigovic, ANZ 18
9. Data and Integration as Strategic Priorities 20
10. Q&A with Radish Singh, EY 24
11. Focused AI Deployment, Not Experimentation 26
12. Q&A with Doron Goldbarsht, Financial Integrity Hub 28
13. Substance Over Form: Evolving Regulatory Expectations 30
14. Implications and Outlook 33

Executive Summary

For more than half a decade, the AML Tech Barometer report has documented a fundamental shift in how financial crime operates across the region. Early editions focused on technology adoption and capability uplift. Subsequent reports documented acceleration, driven by digitisation, sanctions shocks, and a sharp rise in fraud and scams. By 2026, that evolution has reached a more decisive stage. The character of financial crime has changed.

What once appeared as a collection of related risks now operates as a converged threat environment. Fraud, cyber intrusions, scams, sanctions evasion, and money laundering no longer sit separately; they reinforce one another, compressing timelines and exploiting organisational seams. Criminal activity unfolds as a continuous chain, often spanning multiple channels and jurisdictions before traditional controls can meaningfully intervene.

This convergence is most visible in the industrialisation of scams. Scam-related activity has become a dominant entry point into the financial crime system, leveraging mule networks, instant payment rails, virtual assets, and cross-border laundering mechanisms. These cases rarely present as isolated incidents. Instead, they combine social engineering, account compromise, and rapid fund dispersion in ways that overwhelm sequential, siloed control frameworks.

Mule networks remain the critical infrastructure enabling this activity. Despite sustained regulatory attention, mule recruitment has increased rather than declined, driven by automation and increasingly sophisticated incentive and coercion models. In many cases, mule activity is no longer a downstream consequence of fraud or other illicit activities, but a pre-positioned component of scam design – further exposing the limits of control models that assume risks can be addressed one function at a time.

Geopolitics has intensified these pressures. Sanctions risk has expanded well beyond traditional screening functions, intersecting with trade finance, re-export hubs, and complex supply chains. Dual-use goods, tariff evasion, and opaque ownership structures have drawn trade activity firmly into the financial crime risk perimeter. Virtual assets, meanwhile, have become an embedded layer within this ecosystem, with stablecoins in particular compressing laundering timelines and complicating attribution and recovery.

Against this backdrop, the 2026 AML Tech Barometer identifies five strategic imperatives that increasingly distinguish institutions able to operate effectively in a converged threat environment from those that cannot:

Break the siloes. Treating AML, fraud, cyber, and sanctions as distinct risk domains no longer reflects how financial crime operates. Leading institutions are moving toward unified intelligence, governance, and response frameworks that enable risks to be detected and acted upon across domains in near real time. This year's survey data shows that 'Integrating AML and Anti-Fraud' is a business priority for 29.4% of institutions, but beyond individual firms, breaking siloes across the industry leads to a network effect with far greater benefits.

Fix the data foundations. Convergence has exposed the cost of fragmented data, legacy platforms, and inconsistent data quality across KYC, CDD, transaction monitoring, and case management. While this challenge is most acute in transaction monitoring — with 41.8% of institutions citing data quality as the biggest hurdle for monitoring systems — its impact extends across detection, investigation, and decision-making. Without modernised, real-time, cross-domain data foundations, even advanced analytics struggle to deliver meaningful outcomes.

Reframe sanctions and trade risk. Sanctions exposure and trade-based financial crime are no longer compliance adjacencies. They are core financial crime risks, increasingly intertwined with fraud, AML, and network-based laundering activity, and must be governed and monitored accordingly.

Deploy AI with discipline. Advanced analytics, AI, and network-based detection are now prerequisites for operating at speed and scale. But accelerating adoption without corresponding investment in explainability, model governance, and trust frameworks risks creating new vulnerabilities rather than closing existing ones.

Scale collaboration. Public-private partnerships and cross-border information sharing have moved beyond experimentation. In a converged threat environment, collaboration must function as infrastructure – embedded, repeatable, and operational – rather than as a series of pilots or ad hoc initiatives.

Though these priorities are interdependent, progress in one area rarely compensates for weakness in another.

The 2026 AML Tech Barometer points to a widening gap between

strategic intent and operational execution. Board-level awareness of convergence risk is rising, but delivery remains uneven. A small but growing group of institutions is beginning to coordinate fraud, AML, cyber, sanctions, and trade risk in near real-time. Many others remain constrained by fragmented data, ageing systems, siloed governance, and persistent skills shortages. In fact, the size of the organisation plays a key role, with large Tier 1 institutions often having less cross-departmental coordination due to the inherent size of their siloes.

The conclusion is straightforward. Incremental improvement is no longer enough. Effectiveness now depends on intelligence-led orchestration – integrating data, analytics, governance, and response across risks that criminals already treat as one. Institutions that adapt at the pace the environment demands will be better positioned to combat existing and emerging fraud attacks and money laundering schemes.

Those that do not may find that the operating assumptions underpinning their control frameworks have already expired, which will make catching up exponentially more difficult and costly.

Introduction

Fraud and financial crime in the Asia-Pacific region are changing faster than the systems designed to contain them. In a region defined by scale, cross-border connectivity, and rapid digitisation, the gap between threat and control is widening.

Over the past decade, financial institutions across the region have invested heavily in financial crime controls. Sanctions screening is near-universal. Advanced analytics and AI-enabled monitoring are now widely deployed, though their maturity and effectiveness vary sharply across institutions and markets. These investments have improved coverage and efficiency. What is increasingly being questioned, however, is whether they have changed outcomes – and whether they remain aligned with the way financial crime now operates.

Fraud and financial crime have shifted from episodic, linear processes to dynamic, interconnected networks. Scams have emerged as a principal entry point into the financial system, feeding mule networks, instant payments, virtual assets, and cross-border laundering flows. Risks once treated as adjacent – fraud, cyber intrusion, money laundering, sanctions evasion, and trade-based abuse – are now tightly intertwined. Timelines have shortened. Boundaries between typologies have blurred. Controls built for sequential processes are being tested by activities that operate in parallel.

The external environment has become more demanding. Geopolitical tensions have expanded the reach and complexity of sanctions, drawing trade finance, re-export hubs, and opaque ownership structures into the centre of financial crime risk. Virtual assets are no longer peripheral; they are an embedded layer of both legitimate finance and money laundering activity. From an AML/CTF perspective, multi-currency, non-custodial, and interest-bearing stablecoins enable rapid cross-border value movement that materially complicates attribution, jurisdiction, and control.

Environmental and ESG-linked crimes have attracted growing enforcement attention, even as detection remains uneven. Regulatory expectations, meanwhile, are shifting from formal compliance towards demonstrable effectiveness.

These shifts towards increased connectivity in financial crime turns isolated threats into systemic challenges. Together, they compress response times, expose organisational fragmentation, and raise the cost of failure. Financial crime increasingly presents not as a series of problems to be addressed in sequence, but as a system – adaptive, cross-border, and adept at exploiting gaps between institutions, data, and controls.

The 2026 edition of the AML Tech Barometer examines how institutions across Asia-Pacific are responding to this shift. Drawing on perspectives from banks, regulators, and industry practitioners, it assesses where risk is intensifying and whether existing operating models, technologies, and governance arrangements remain adequate.

With financial institutions having to play within predefined regulatory rules, and criminals having an open playbook giving them the edge, the question is straightforward. As financial crime becomes faster, more connected, and deeply embedded within legitimate systems, can institutions adapt at the same pace?

About the 2026 AML Tech Barometer

The AML Tech Barometer is a joint longitudinal research initiative by Regulation Asia and NICE Actimize that examines how financial institutions and their senior leadership across Asia-Pacific are responding to an increasingly complex financial crime environment. First published in 2021, the Barometer tracks not only the adoption of technology in AML and financial crime risk management, but the broader evolution of institutional capability as threats, regulations, and operating models change.

Early editions focused on foundational questions: whether institutions had the systems and processes needed to meet baseline regulatory expectations. As financial crime has become increasingly digitised, networked, and closely tied to geopolitics, the Barometer has evolved to assess how effectively institutions integrate fraud, AML, cyber, sanctions, and trade-related risks into a coherent control framework.

The Barometer is diagnostic rather than prescriptive. It does not rank institutions or advocate a single operating model. Its purpose is to identify where industry practice is converging, where gaps persist, and where institutional assumptions no longer align with the realities of the threat environment.

Continuity is a core feature. A consistent set of themes is carried forward year-on-year to allow comparison across time, markets, and institution types, while new areas of focus are introduced as risks evolve. Recent editions have placed greater emphasis on risk convergence, the governed use of advanced analytics and AI, sanctions and trade exposure, and the role of collaboration and information sharing in disrupting financial crime networks.

The 2026 edition reflects a point of transition. Institutions are no longer judged primarily on whether they have invested in technology, but on whether those investments translate into practical outcomes. Regulators are placing greater emphasis on effectiveness, data quality, and cross-domain risk management.

The Barometer is written for those who shape and scrutinise financial crime strategy: banks benchmarking maturity; regulators and supervisors assessing industry capability; financial intelligence units and enforcement agencies tracking typology evolution; and policymakers confronting the economic and geopolitical consequences of illicit finance. It aims to provide a clear view of a region caught between accelerating innovation and increasingly complex threats – and a financial sector under pressure to keep pace.

Methodology

The findings in this report are drawn from a combination of quantitative and qualitative research conducted across the Asia-Pacific region as part of the ongoing AML Tech Barometer study.

Primary data was collected through a structured survey of 133 financial crime professionals from banks, securities firms, wealth managers, payment service providers, fintechs, and other regulated entities operating across the region. Respondents include a mix of global, regional, and domestically focused institutions, capturing differences in scale, complexity, and regulatory exposure.

A core set of survey questions has been retained year on year to support comparability and identify directional change in areas such as technology adoption, operating models, governance structures, and perceptions of financial crime risk. These are supplemented by targeted questions introduced to reflect emerging developments. In 2026, these focus in particular on risk convergence across fraud, AML, cyber, sanctions, and trade; the use of advanced analytics and AI; and approaches to cross-domain coordination and information sharing.

Survey data is supplemented by in-depth interviews with senior practitioners, technology leaders, and public-sector stakeholders across the region. These interviews are used to contextualise findings, test assumptions, and explore areas where quantitative responses alone cannot capture operational or supervisory complexity.

The analysis prioritises direction and pattern over point precision. Percentages illustrate shifts and contrasts in practice rather than market-wide measurement, with divergent responses treated as a signal reflecting uneven maturity and operating environments. Findings reflect conditions at the time of research and are intended to inform strategic judgement rather than tactical implementation.

The Evolving Threat Landscape

From Fragmented Risks to a Converged Threat Environment

Over the past five years, the AML Tech Barometer has documented a steady expansion in both the scale and sophistication of financial crime across Asia-Pacific. What distinguishes 2026 is not the sudden appearance of new threats, but the degree to which existing ones now operate together. Fraud, cyber intrusion, scams, sanctions evasion, and money laundering have converged into a single threat environment – one that exploits speed, scale, and organisational seams.

Earlier editions of the Barometer treated these risks as adjacent. That distinction is now steadily eroding. By 2025, many practitioners reported that suspicious activity investigations frequently involved multiple risk typologies within the same case rather than a single predicate offence. The latest findings indicate that this trend has continued, reinforcing the shift toward multi-risk convergence.

The practical consequence is a collapse of sequence. Criminal activity now unfolds as a continuous chain rather than a series of discrete events, with entry points, monetisation, and laundering tightly integrated across channels, products, and jurisdictions. In such an environment, delay is risk, and fragmentation is exposure.

“The fundamental threats are persistent; it’s the criminal methodologies that change,” observes Milan Gigovic, Head of Financial Crime Threat Management at ANZ. “On the back of this, we see professional money laundering groups being hired to move the proceeds, leading to a convergence of different threats that makes traditional transaction monitoring much harder.”

Scams as the Primary Entry Point

Scams have emerged as the dominant entry point into the financial crime system across much of Asia-Pacific. Over successive Barometer cycles, scam-related activity has consistently ranked as the fastest-growing driver of suspicious-transaction reporting.

Between 2023 and 2025, approximately 65–70% of institutions reported a material year-on-year increase in scam-linked alerts and cases, with the latest data suggesting further growth, particularly in retail and digital payments environments. A combined 70.1% of respondents observed either a 'Significant Increase' (41.6%) or 'Slight Increase' (28.5%) in suspicious activity related to fraud and scams over the past 12 months.

These cases rarely present as isolated incidents. Instead, they combine social engineering, account compromise, mule recruitment, and rapid fund dispersion – often within hours of initial contact with a victim. In Hong Kong, regulators have observed that fraud now acts as the predicate offence in more than 70% of money-laundering investigations. Comparable patterns are emerging across additional jurisdictions in 2026.

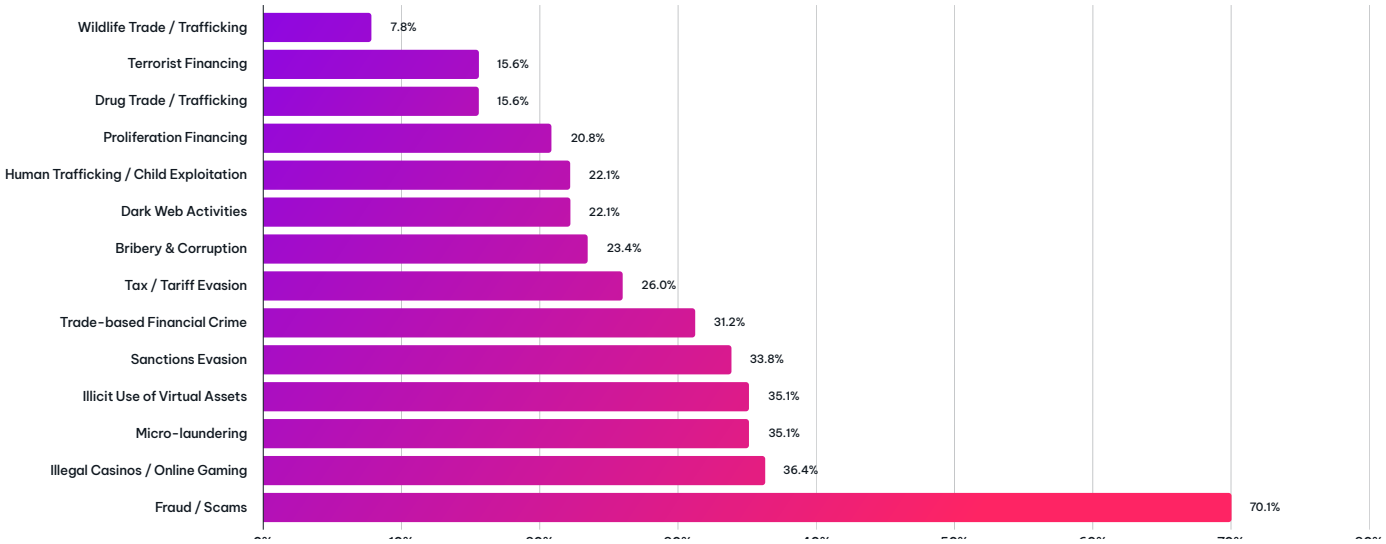
What defines the current scam landscape is its level of industrialisation. Scam operations increasingly resemble coordinated production systems, with distinct roles responsible for recruitment, victim engagement, payment execution, laundering, and cash-out. The increasing use of advanced technology is further compounding this threat.

"Technology, especially AI, has dramatically increased the efficiency of these scams," said Sungyong Kang, Criminal Intelligence Officer at INTERPOL. "Criminals use data from the dark web or open sources to create highly tailored "spear phishing" tactics. Before AI, this was too costly and time-consuming to do at scale. Now, with AI and deepfake technologies, criminals can target a much larger number of people with highly convincing, personalised frauds, which significantly increases their success rate."

The United Nations Office on Drugs and Crimes (UNODC) estimates that scam-related losses targeting victims in East and Southeast Asia reached USD 18–37 billion in 2023, much of which ultimately passed through regulated financial institutions at some stage of the laundering cycle. Updated regional estimates for 2026 are expected to exceed prior levels.

Proceeds are typically routed through instant-payment rails, virtual assets, OTC brokers, and, in some cases, trade-linked channels before traditional controls can meaningfully intervene.

Areas of Increased Activity in Suspicious Activity Reporting



Mule Networks as Enabling Infrastructure

Mule networks remain the critical infrastructure enabling financial crime. Despite sustained regulatory attention, mule recruitment has scaled – supported by automation, online marketplaces, and increasingly sophisticated incentive and coercion models.

By 2024, approximately 60% of retail banks in Hong Kong reported active deployment of network-analytics tools specifically to identify mule-account networks, more than double the adoption observed three years earlier. In 2026, adoption continues to expand, though this capability still lags the threat. Across Asia-Pacific, only 31.5% of institutions with automated systems report having network analytics capabilities, and just 18.1% have prioritised it as a technology focus for the coming year.

The 2026 findings suggest that mule activity is no longer merely a downstream consequence of fraud. It is increasingly pre-positioned, with accounts prepared in advance and activated the moment funds are obtained. Institutions report a rising proportion of cases in which mule accounts exhibit risk indicators before scam proceeds enter the system – further undermining sequential control models that assume risk can be intercepted at discrete stages.

As Matthew Field, APAC Market Director Anti-Money Laundering at NICE Actimize, observes, "Mule-enabled laundering is rarely linear. Funds are routed through pre-positioned accounts, rapidly dispersed across multiple accounts and institutions, and often consolidated or laundered onward within hours. By the time a transaction is flagged, activity has already moved beyond point in time controls — effective disruption depends on seeing the network, not the individual transaction."

Sanctions, Trade, and Geopolitics

Geopolitical tensions have intensified financial crime risk at the intersection of sanctions, trade finance, and supply chains. Sanctions exposure and tariff avoidance now extend well beyond conventional name-screening, reflecting the growing prevalence of dual-use goods, re-export hubs, and complex ownership and routing structures.

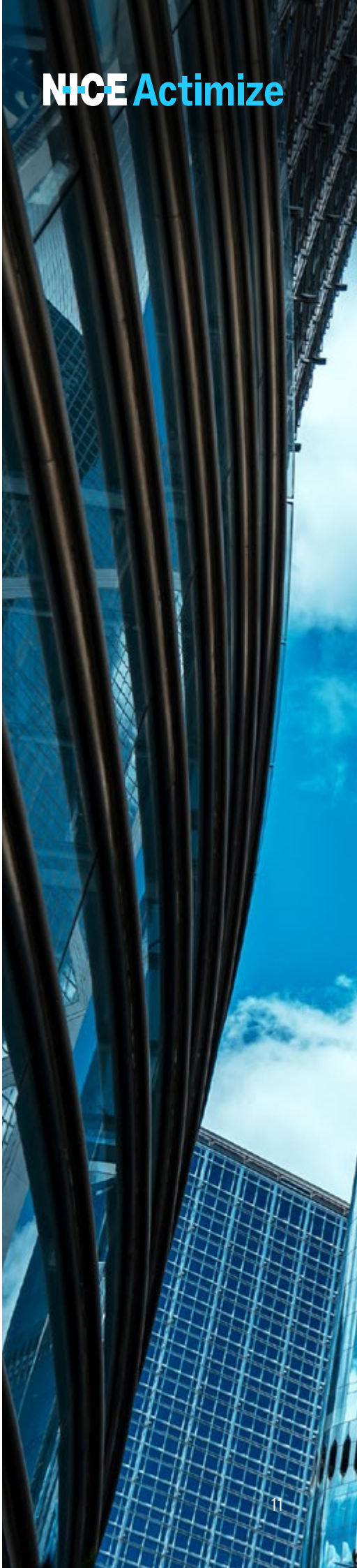
Across the 2023–2025 Barometers, trade-based money laundering (TBML) consistently ranked among the top five areas of increased suspicious activity, with around 30% of institutions reporting a moderate or significant rise in TBML-related risk over the previous 12 months. The 2026 survey shows this trend continuing, with a combined 31.2% of respondents reporting an increase in TBML-related suspicious activity. TBML is increasingly cited alongside sanctions evasion within the same investigations rather than as a standalone issue.

In practice, these risks are inseparable, even where institutional responsibility remains divided across functions and business lines. Trade activity, once treated as a specialist compliance concern, now sits firmly within the core financial crime risk perimeter, reshaping what effective investigation requires.

As Matthew Field observes, "Where trade, sanctions, and laundering risks converge, investigations can no longer be handled in isolation. The ability to connect trade documentation, transaction behaviour, and sanctions exposure within a single investigative view is becoming a core competency rather than a specialist add-on."

Virtual Assets as an Embedded Layer

Virtual assets have moved from the periphery to the centre of the criminal toolkit. Cryptocurrency-related activity has ranked as the first or second driver of increased suspicious reporting across the past three Barometer cycles. The data collected for this latest edition shows that this pattern has consolidated rather than reversed: a combined 35.1% of respondents reported year-on-year growth in crypto-linked suspicious activity during the past 12 months.



Unlike earlier years, crypto exposure is no longer confined to customers with explicit digital-asset profiles. Virtual assets increasingly function as an intermediary layer between fraud proceeds and the traditional financial system, compressing laundering timelines and complicating attribution and recovery.

Persistent and Emerging Vulnerabilities

Some risks have proved stubbornly persistent. TBML, which appeared to stabilise in parts of the region earlier in the decade, is resurfacing in altered form – most notably through sanctions circumvention, tariff avoidance, and increasingly opaque supply-chain structures. Environmental and ESG-linked crimes, including illegal logging, wildlife trafficking, and forced labour, continue to be materially under-detected. Fewer than 15–20% of institutions reported improved detection in 2024–2025, despite growing regulatory scrutiny, with the survey data indicating little change. Only 7.8% of respondents reporting an increase in suspicious activity related to wildlife trafficking and 22.1% for human trafficking.

Alongside these enduring risks, new techniques are beginning to scale. Synthetic identity creation and deepfake-enabled impersonation, once marginal, are now testing onboarding and authentication controls. Several jurisdictions reported initial detection of deepfake-assisted fraud during onboarding and account maintenance in 2025. By 2026, these methods appear to be moving beyond experimentation, with organised groups increasingly incorporating them into repeatable fraud and account-compromise strategies.

A Converged Threat Environment

Taken together, the 2026 findings point to a simple reality. Financial crime in Asia-Pacific no longer resembles a collection of related risks managed in sequence. It functions instead as a converged threat environment, exploiting speed, scale, and organisational fragmentation.

Institutions that continue to manage fraud, AML, cyber, sanctions, and trade risk in isolation are becoming more exposed. Those beginning to integrate intelligence, data, and response across these domains appear better positioned, though they remain the exception rather than the rule – a pattern the 2026 data shows little sign of reversing.

In such an environment, effectiveness depends less on adding new layers of control than on re-architecting how risk is understood, detected, and acted upon across the organisation. The collapse of old boundaries is already a fact. The open question is whether institutional operating models have kept pace.

Interview with Sungyong Kang
Criminal Intelligence Officer, Financial Crime and Anti-Corruption Center INTERPOL

Sungyong Kang discusses the industrialisation of scams into a global threat, INTERPOL's multi-pronged strategy to combat transnational organised crime, the challenges posed by high-speed payments and virtual assets, and the critical need for a cultural shift within financial institutions.

The views expressed are those of the interviewee and do not represent the official views of the INTERPOL or any other organisation.

How has the financial crime landscape evolved in the last 12 to 18 months, and what do you see as the biggest threat today?

Sungyong Kang: The most significant threat we see is the evolution of scams. While not a new crime, the scale and damage are bigger than ever, affecting more countries and becoming a major global threat. What's changed is that scams have become industrialised. Criminals are dividing labour – we call "crime-as-a-service" – where one criminal group provides services to another.

This industrialisation has led to the rise of scam compounds, which are much larger than simple call centres. This is no longer just a financial crime; it has become a human rights issue involving human trafficking, torture, rape, and even murder. We are also seeing these scam compounds expand beyond Southeast Asia into regions like the Middle East, Africa, and Latin America, making it a truly global problem. Even as we go after them in one region, they pop up in another.

Technology, especially AI, has dramatically increased the efficiency of these scams. Criminals use data from the dark web or open sources to create highly tailored "spear phishing" tactics. Before AI, this was too costly and time-consuming to do at scale. Now, with AI and deepfake technologies, criminals can target a much larger number of people with highly convincing, personalised frauds, which significantly increases their success rate.

Given the rise of these transnational organised crime groups, what is INTERPOL's strategy to combat them?

Sungyong Kang: We recently adopted a new strategy at our General Assembly to specifically target these transnational groups. While the specific standard operating procedures are still being developed, we are building on work we already do. A key part of our strategy is helping member countries build their own capacity.

For example, we recently held a five-day conference to help Southeast Asian countries to establish their own anti-scam centres. We invited senior-level officials from their police forces, central banks, FIUs, and telecommunication authorities to learn from countries that already have successful anti-scam centres. The goal is to provide strategic and policy-making support so they can build a better system to go after scams.

Operationally, we continue to work with member countries to go after scam compounds through initiatives like Operation HAECHI, which is funded by the Korean National Police Agency. This operation targets cyber-enabled financial crime and has been a key part of our efforts against scam compounds. We will continue to support our member countries on the ground through these coordinated operations.

What are the key challenges you see from the exploitation of high-speed payments and virtual assets by bad actors, and what are the solutions?

Sungyong Kang: The speed of fintech and virtual assets makes it extremely difficult for law enforcement to follow the money, especially across borders. To fight high-speed money laundering, we need high-speed cooperation. This requires swift information sharing and swift enforcement.

Domestically, countries are trying different methods. Singapore co-locates financial institution staff with police in its anti-scam centre for on-the-spot information sharing. Malaysia has a system called

(Sungyong Kang interview continued)

PayNet that can trace domestic transactions. Korea uses an integrated system to automatically deliver police alerts to financial institutions.

For cross-border transactions, the challenge is greater. A SWIFT recall might not always be fast enough. To help, INTERPOL uses its police-to-police channel, I-GRIP, to relay victim complaints from one jurisdiction to another. This allows police in the beneficiary jurisdiction to inform the bank about the incoming fraudulent funds and encourage a voluntary suspension of the account until a formal recall or legal order arrives.

However, we often have to rely on the voluntary actions of financial institutions, which is not always enough. We need stronger legal powers. The FATF recommendations encourage countries to give their FIUs administrative power to issue suspension orders on suspicious accounts. This is much faster than a criminal restraining order.

We need all countries to adopt and use these powers. Without them, we are stuck with the mutual legal assistance (MLA) process, which can often take longer than the temporary suspension period during which a bank is allowed to hold suspect funds.

Public-private partnerships are essential in this fight. Information sharing has historically been a one-way street, with the private sector reporting to public authorities. It needs to be a two-way street. Public authorities should share their data to help the private sector do their job better, especially since we are asking them to perform a police function by detecting crime.

> **"Information sharing has historically been a one-way street, with the private sector reporting to public authorities. It needs to be a two-way street."**
>
> **Sungyong Kang, INTERPOL**

INTERPOL, as the only global repository of crime intelligence, aims to provide certain data that is useful to the private sector for detecting and preventing crime. In the end, the data needed by the private sector to fight against cross-border crime is not just domestic data but global data.

What is your key message to financial institutions that are on the front lines of this battle?

Sungyong Kang: Financial institutions need to change their culture and mindset from the top down. They cannot just wait for new laws, stronger enforcement, or additional liabilities to be imposed on them. A voluntary cultural change is needed.

Too often, we see financial institutions prioritise the risk of a civil lawsuit from an account holder over the risk of AML/CFT enforcement. They let suspicious transactions go through because they are afraid of being sued for suspending an account. But, these scams are not just simple financial crimes anymore; they are linked to horrific human rights abuses. So the culture needs to shift.

This can be demonstrated through the words and actions of the CEO and senior leadership, through training, and – most crucially – by revising KPIs. Performance should not just be about profit or the number of clients; it should also be about how much money was stopped and how many victims were helped.

If financial institutions change their mindset and voluntarily take a stronger stance, it will greatly help our collective job of protecting victims and fighting these devastating crimes.

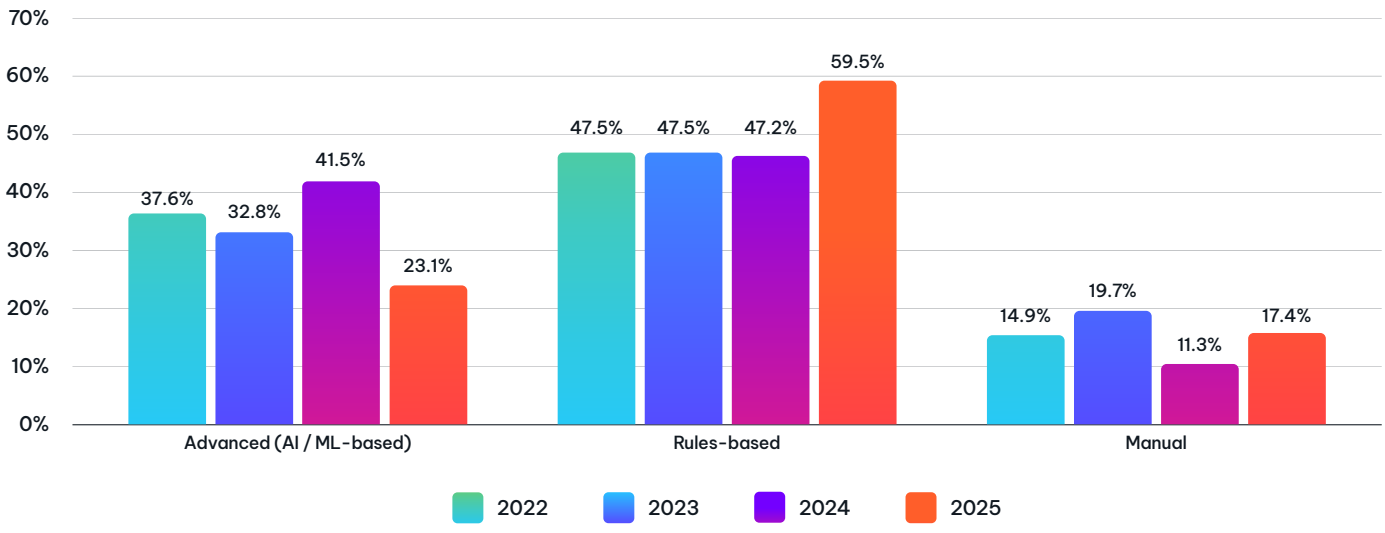
Financial Crime and Technology Priorities

Alignment, Trade-offs, and Blind Spots

As financial crime risks converge, institutions across Asia-Pacific are being forced to make more explicit choices about where to focus investment, management attention, and organisational change. The 2026 AML Tech Barometer shows that while priorities are shifting in the right direction, alignment between perceived risk, technology investment, and operating-model change remains uneven.

Most institutions now acknowledge that incremental enhancements to legacy controls are insufficient. Recognition, however, has not always translated consistently into execution. Competing demands, organisational inertia, and uncertainty over evolving supervisory expectations continue to slow the transition from siloed compliance functions to integrated risk management.

How Respondents Describe FI's Financial Crime Risk Management Systems



A key finding from this year's survey is a potential market correction or 'flight to safety' in technology systems. The proportion of institutions describing their systems as 'Advanced' (i.e. reliant on AI/ML) has fallen from 37.6% to just 23.1%. Conversely, those describing their systems as 'Rules-based' has increased from 47.5% to 59.5%.

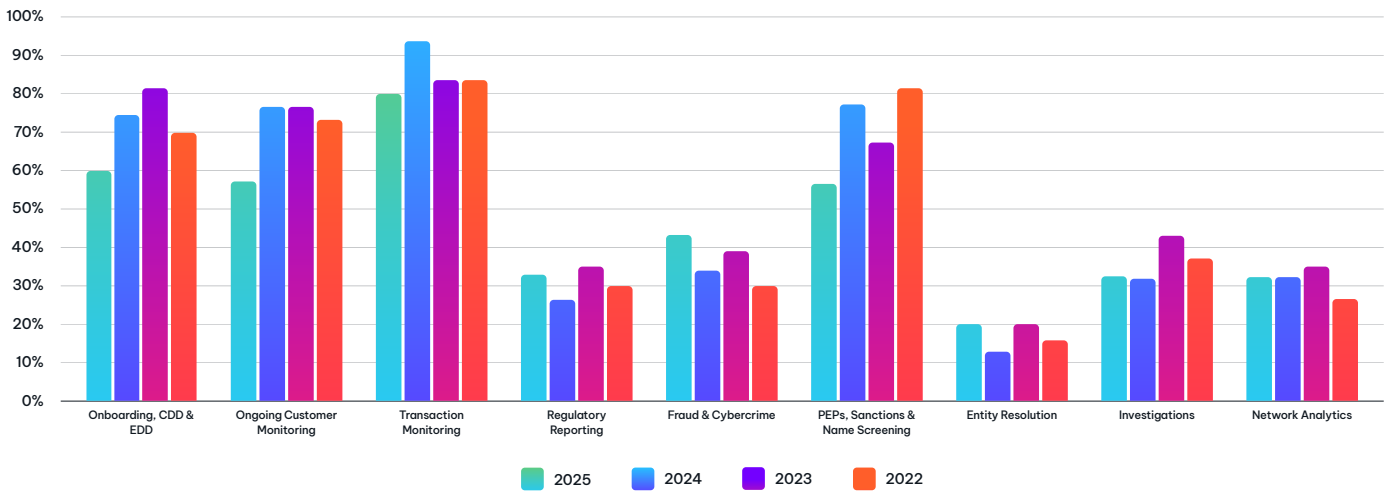
This apparent regression does not necessarily signal a failure of AI, but rather a shift from a period of broad experimentation to one of disciplined, governed deployment. The industry appears to be moving past the initial hype cycle and confronting the practical realities of implementing advanced technology. Several factors appear to be driving this trend:

- **Regulatory scrutiny and need for explainability:** As regulators increasingly focus on substance and effectiveness, the ability to explain and defend a system's logic has become paramount. Opaque "black box" models present a significant regulatory risk. Rules-based systems, while less dynamic, offer a clear, auditable trail of decision-making that is easier to validate and defend.

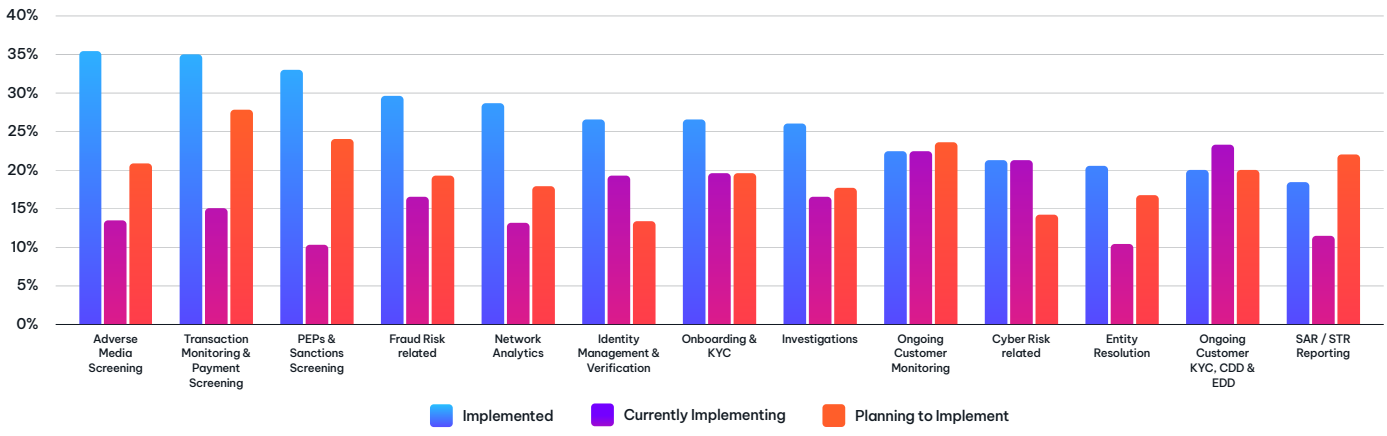
- **A focus on foundational stability:** Many institutions have learned that layering advanced analytics on top of weak data foundations yields poor results. The priority for many has shifted to fixing core data quality and integration issues – a prerequisite for any successful AI implementation. A stable, well-understood rules-based engine provides a reliable baseline from which to build.
- **The emergence of a hybrid reality:** This year's survey attempts to capture greater nuance of current operating models. Rather than a wholesale replacement, we find that institutions are embedding AI capabilities into specific parts of a rules-based workflow. For example, a rules-based system might still generate the initial alerts, but an AI model is then used for intelligent alert triage or false positive reduction. The survey data shows that even among those who classify their systems as 'Rules-based', the average rating of their system's advancement is 5.5 on a 10-point scale, indicating that many are not purely static.

This shift represents a maturation of the market. Institutions are no longer adopting AI for its own sake, but are instead making pragmatic choices, prioritising governed, use-case-specific deployments that deliver measurable value without introducing unacceptable governance or regulatory risk.

Operational Areas Covered by "Advanced" or "Rules-based" Systems



AI/ML Implementation Status



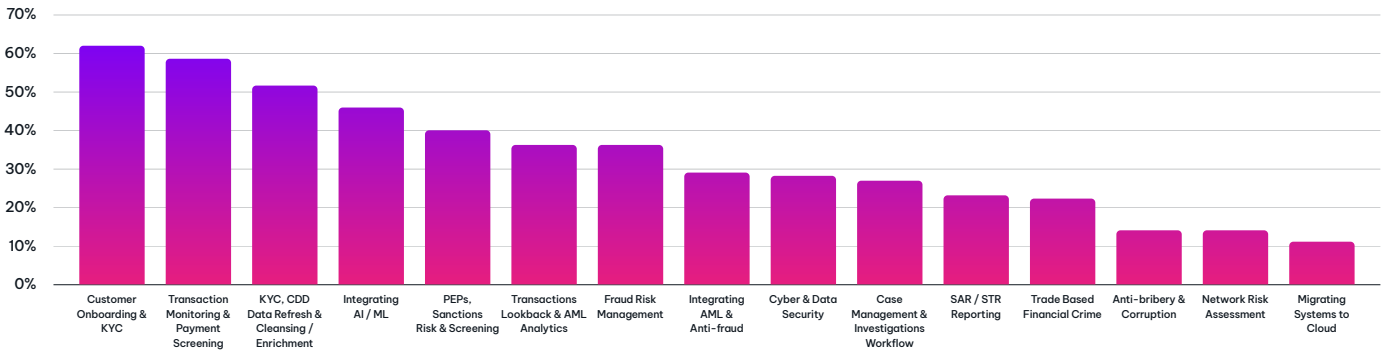
Effectiveness Over Expansion

While efficiency remains a key driver for financial institutions, the question in 2026 is whether existing systems are adequately effective in detecting real threats and keeping pace with the speed, volume, and complexity of financial crime. This is reflected in the top use cases practitioners believe could be enhanced by AI, with 'False Positive Reduction' (66.7%) and 'Suspicious Activity/Anomaly Detection' (64.1%) ranking highest.

Institutions increasingly cite optimisation – rather than wholesale replacement – as their primary near-term objective, focusing on reducing false positives, improving investigative context, and shortening response times in high-velocity cases such as scams and mule activity.

This recalibration reflects both budgetary constraint and regulatory signal. Regulators across the region are placing greater emphasis on outcomes, data quality, and demonstrable risk mitigation than on the mere presence of advanced tools. As a result, institutions are prioritising initiatives that improve end-to-end performance over those that simply expand functional coverage.

Financial Crime Business Priorities (2025-2026)



Financial Crime Technology Priorities (2025-2026)

Interview with Milan Gigovic
Executive and Head of Financial Crime Threat Management
ANZ

Milan Gigovic discusses ANZ's technology and intelligence-led approach to financial crime, the power of its data asset and AI tools, and the need for public-private partnerships as essential weapons in the fight against sophisticated criminal networks.

How has the financial crime landscape in Australia evolved in the last 12-18 months, and what are the key threats facing financial institutions today?

Milan Gigovic: The fundamental threats remain persistent; it is the methodologies that evolve. The criminal profits generated from illicit commodities continue to be a major focus for us. This includes the proceeds of illicit tobacco, which is a multi-billion-dollar annual problem, as well as the illicit drug market, where supply and demand is at record highs. On the back of this, we are seeing a convergence of traditional money laundering, fraud, and scams, with the illicit profits generated from these crimes being moved by the same professional money laundering networks.

Criminals are exploiting information sharing barriers between financial institutions, diversifying their illicit proceeds across multiple banks, layering funds domestically, and then using third parties to move money offshore. It's becoming more complex. The art is understanding how criminal methodologies are evolving, which requires having the right people capability, enriched data, and advanced technology platforms in place to combat these threats. This enables us to detect and respond swiftly, and, importantly, leverage both private-to-private and public–private partnerships to enhance disruption opportunities.

What is ANZ's strategy behind the bank's financial crime detection capabilities?

Milan Gigovic: We made a strategic decision over a decade ago, before any of the major regulatory fines in Australia, to build our own internal data asset. We call it our Financial Crime Data Repository (FCDR). It underpins most of our tooling and algorithms and today it holds over eight years of data – tens of billions of transactions with over 1,500 unique data points. The tools we have built on top of this enriched data asset enables us to test any hypothesis in real-time and we use the results to determine whether our controls need to be enhanced and importantly it enables us to provision timely actionable intelligence.

This intelligence ecosystem has also enabled us to divest from traditional tools and rules-based transaction monitoring solutions and instead design and deploy what we call "dynamic algorithms". This started in 2014 in partnership with AUSTRAC and the Australian Federal Police (AFP) to combat child exploitation. We found we could combine our tradecraft and data knowledge with intelligence from the regulator and law enforcement to be much smarter about detection.

We went from huge false positives to lower alert volumes with higher yield, detecting the right risks and sharing that intelligence with partners in industry and government. We now have over 25 dynamic algorithms aligned to specific typologies like child exploitation, shadow banking, illicit tobacco, extremism, sanctions circumvention, fraud, and networked money laundering. These algorithms have a very high true positive conversion rate, allowing us to focus on what matters. We have also deployed several ANZ proprietary algorithms and tools at another bank in Australia which has helped them uplift their controls, reduce false positives and has led to better quality reporting and intelligence outcomes.

How are you using artificial intelligence to augment your team's capabilities and improve efficiency?

Milan Gigovic: We have introduced AI in the form of what we call the 'ULTRON' tool which stands for 'Universal Layered Threat Response Organisation and Narration'. When we are investigating a customer, an analyst can, at the click of a button, get a written dossier on what that customer has been doing, going back eight years. It stitches everything together and presents it as a dashboard, highlighting key risks and importantly provides a written narrative of the customers activity.

The way we use generative AI is not as a decision-maker, but as a tool, or what I'd coin an 'executive assistant'. It

(Milan Gigovic interview continued)

does all the manual, 'swivel chair' labour of going into different source systems, which means our investigators don't have to spend time trawling through data and bank statements but rather focus on analysis and informed decision making. What used to take us on average 45 minutes now takes us a few seconds and if you think about the amount of alerts we as an industry work it has made a significant difference.

ULTRON also presents insights in a way that isn't possible manually. It effectively allows our investigators to make better informed risk decisions due to the enriched insights presented and it immediately enables investigators to focus on analysis and making a decision: Do we report them? Do we escalate? Do we refer to law enforcement? It has been a game-changer.

How is collaboration through public-private partnerships changing the game in Australia?

Milan Gigovic: This is the new frontier. We are very lucky to have a progressive and capable regulator in AUSTRAC, and we have the innovation mandate to do things differently through the AUSTRAC-led Fintel Alliance. This means fusing our data together and deploying algorithms over the top to find risks that we simply cannot find working in isolation.

We've already shared our algorithms for networked money laundering, child exploitation, fraud, and extremism with other financial institutions through the Fintel Alliance. More recently, we ran an exercise where we designed a data schema, had six banks contribute their data, and ran an algorithm over the fused dataset to look for domestic child exploitation threats.

That one exercise led to the referral of 10 suspected perpetrators to the AFP led Australian Centre for Combating Child Exploitation (ACCCE). We did the same thing to identify professional money laundering groups, resulting in same-day referrals to law enforcement on risks we were detecting in near real-time. This is what effectiveness looks like in practice.

What have been the tangible outcomes of this collaborative, intelligence-led approach?

Milan Gigovic: The outcomes have been significant. Through these collaborative Fintel Alliance projects, we have seen seizures of cash, firearms, and drugs like methamphetamine and cocaine. We have uncovered the most serious forms of criminal harm, including child exploitation and, more importantly, identified victims who we helped save from serious harm. None of that could be done if we didn't join forces.

> **"The way we use generative AI is not as a decision-maker, but as a tool, or what I'd coin an 'executive assistant'. It does all the manual, 'swivel chair' labour... What used to take us on average 45 minutes now takes us a few seconds."**
>
> **Milan Gigovic, ANZ**

This is our weapon. Because we can provide timely intelligence, law enforcement can act while the criminals are still in the country and the money is still in the account. If they get the intelligence 60 days later, the money is gone, the criminals have moved on, and it makes it harder for law enforcement to disrupt.

As a result of this work, we were the first bank to be asked by the AFP to second a forensic specialist to the ACCCE, and the first bank to second a senior intel team member to co-lead the Fintel Alliance. This demonstrates the power of working together.

Looking forward, what is the next step for the industry and for AML regulation in Australia?

Milan Gigovic: The upcoming changes to the AML Act, some of which comes into effect on 31 March, give us the regulatory safe harbour to do more of this intelligence-led and collaborative work. The next step is to truly amp up public-private information sharing. The Fintel Alliance Collaborative Analytics Hub is the ecosystem where we can do this. We've proven that when we fuse our data and bring our resources together, we get effective outcomes and identify risks we otherwise wouldn't have known about.

Ultimately, I'd also like to see government drive an economic crime strategy. I would love for the government to mandate this collaborative approach. We have the talent and the proven model in Australia. Now it's about building out the ecosystem so we can do this on a daily basis, in real time, and at scale. We need the courage from leadership across government and industry to come together and say, 'We have to do this, and we have to do it now'.

Data and Integration as Strategic Priorities

Investment priorities are increasingly converging on data foundations. Enhancing data quality, improving customer and entity resolution, and enabling cross-domain visibility are now widely recognised as prerequisites for effective use of analytics and AI.

The Barometer suggests a growing consensus that integration – across systems, teams, and risk domains – is no longer an architectural aspiration but a strategic necessity. Institutions that continue to treat integration as a secondary or long-term goal face rising operational friction and diminishing returns on technology spend.

The strategic importance of this is exemplified by ANZ's long-term investment in its data infrastructure. "We made a strategic decision over a decade ago... to build our own internal data asset. We call it our Financial Crime Data Repository (FCDR)," says Milan Gigovic. "This has enabled us to divest from traditional rules-based transaction monitoring and instead design and deploy what we call 'dynamic algorithms'."

Fragmented data remains one of the most persistent constraints on effectiveness and integration. Even where advanced detection tools are in place, inconsistent data standards, weak lineage, and limited interoperability continue to impede timely investigation and escalation – particularly in cases spanning fraud, payments, crypto, and sanctions exposure.

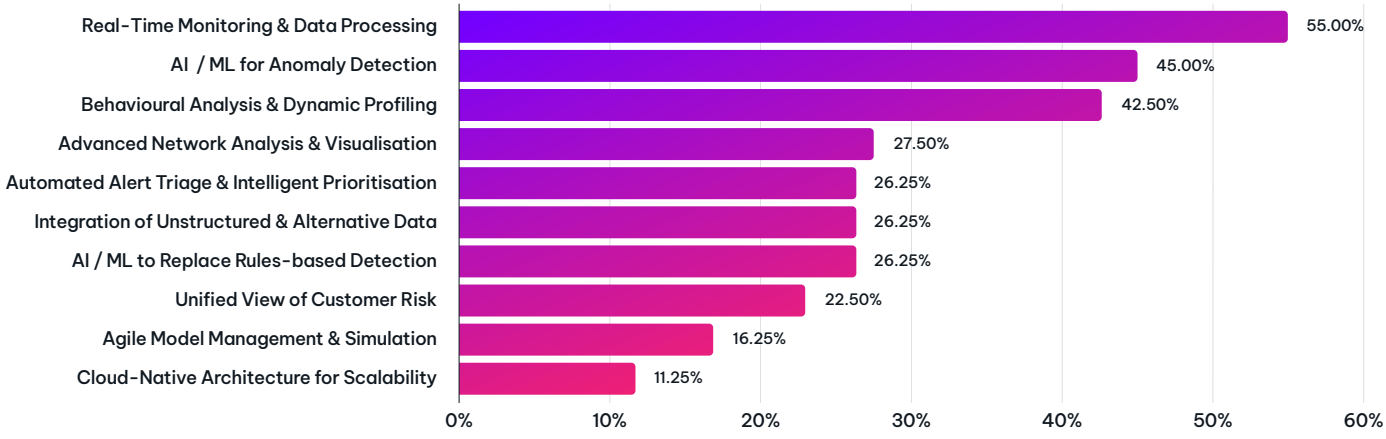
In the research, 'Data Quality & Availability' was cited by 41.8% of respondents as the most significant challenge for their transaction monitoring system – far outpacing any other single challenge. Similarly, 'Data & List Management' was cited as the top challenge for PEPs/sanctions screening systems.

What Practitioners Want from Transaction Monitoring

While AI and machine learning dominate strategic discussions, the research reveals a more fundamental priority for financial crime practitioners. When asked to identify the most essential capabilities for a 'next-generation' transaction monitoring system, the top choice was 'Real-Time Monitoring & Data Processing' (55.0%), higher than both 'AI / Machine Learning for Anomaly Detection' (45.0%) and 'Behavioural Analysis & Dynamic Profiling' (42.5%).

This finding suggests that the ability to detect and intervene instantly is no longer a "nice-to-have" for practitioners – it has become the most critical factor in achieving effectiveness. A sophisticated model that identifies a fraudulent transaction hours after the funds have been moved through a mule network and converted to virtual assets is of little practical use. The priority is clear: speed is the foundation of modern control.

Capabilities Sought from "Next-Gen" Transaction Monitoring System

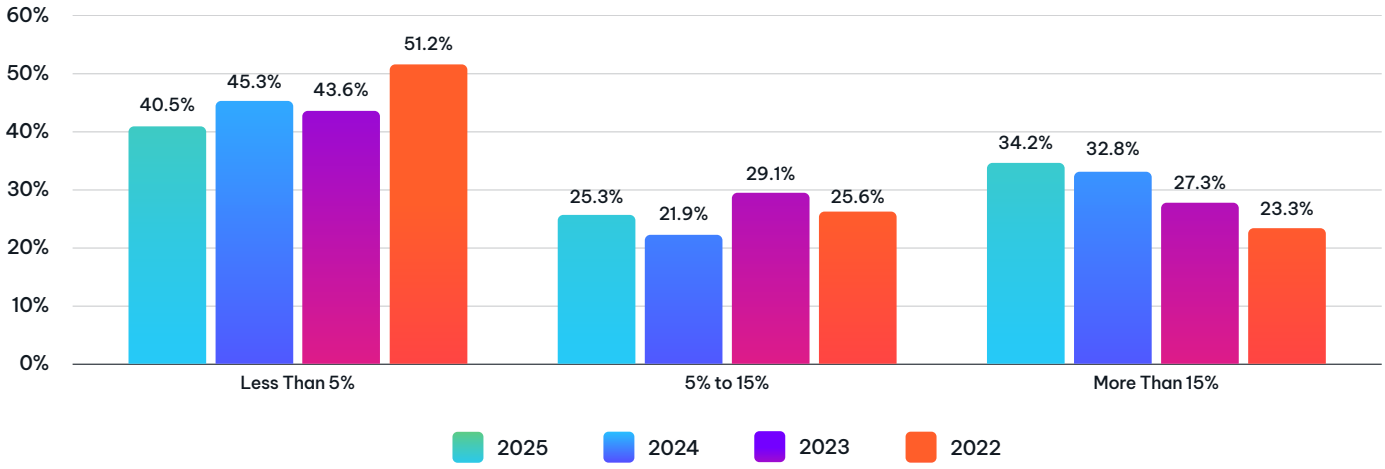


Improvement in Alert Effectiveness

The research has also found that a multi-year trend towards higher-quality alerts and reduced false positives is continuing, demonstrating a clear return on the industry's investment in technology and data refinement. The proportion of institutions reporting high-quality alert outputs (escalating more than 15% of alerts to cases) has reached a four-year high of 34.2% in 2025. This represents a steady and significant improvement from just 23.3% in 2022, 27.3% in 2023, and 32.8% in 2024.

Concurrently, the cohort of institutions with the highest rates of false positives (i.e. escalating fewer than 5% of alerts) has shrunk considerably, from a peak of 51.2% of respondents in 2022 to 40.5% in 2025. This shows a clear, positive shift from low-yield to high-yield alerts, indicating that industry efforts are yielding tangible results in operational efficiency and allowing investigators to focus on genuinely higher-risk activity.

Alert-to-Case Ratios Reported by Respondents (2022-2026)



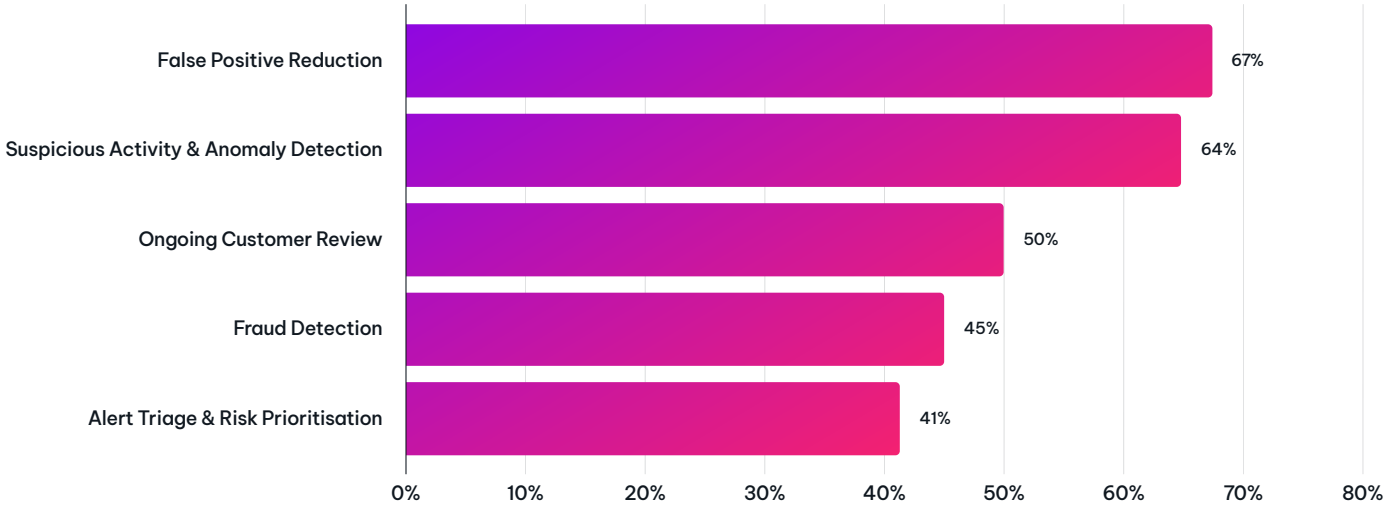
When asked where AI could provide the greatest enhancement to their financial crime programmes, respondents overwhelmingly pointed to the core challenges of operational efficiency and detection effectiveness. Topping the list is "False Positive Reduction", with two-thirds of practitioners (67%) identifying it as a prime use case for AI. This highlights the immense operational burden that legacy systems continue to place on compliance teams.

As Field observes, "early evidence suggests that where AI and predictive scoring are applied with discipline, institutions are not only reducing low-value alerts but also improving detection quality. In several programmes, a higher proportion of escalated alerts are translating into reportable cases, indicating that efficiency gains are being achieved alongside stronger risk identification rather than at its expense."

Radish Singh, Asean Financial Services Risk Consulting Leader at EY, explains the benefit of this shift. "The way transaction monitoring is done today is blunt and rule-based... Going model-based means we write models by learning from vast amounts of data. We are finding that institutions that have gone down this path are seeing two primary outcomes. First, the yield is higher, meaning they see more real anomalies that they didn't see with rule-based engines. Second is efficiency."

Running a close second is "Suspicious Activity/ Anomaly Detection" (64%), indicating a strong desire to leverage AI not just for efficiency, but to improve effectiveness by uncovering novel and more complex criminal typologies that traditional rules might miss. Further down the list, half of the respondents (50%) see significant potential for AI in automating "Ongoing Customer Review", another resource-intensive compliance activity. The application of AI to "Fraud Detection" (45%) and "Alert Triage/Risk Prioritisation" (41%) are also seen as valuable.

Financial Crime Use Cases That Can Be Enhanced the Most Using AI



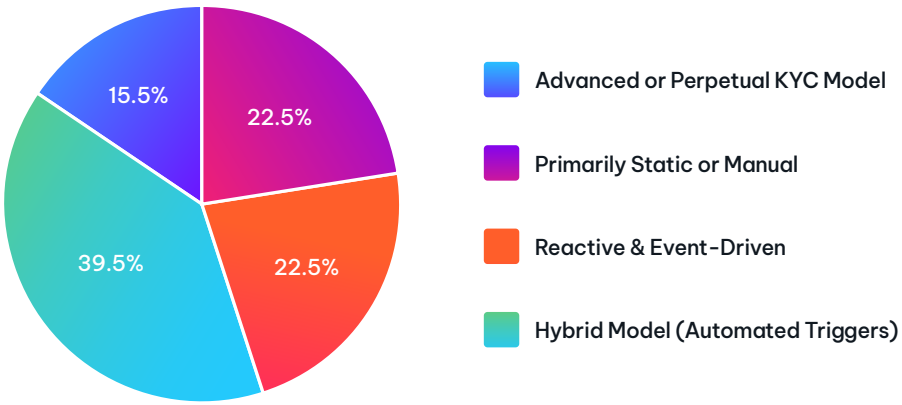
Dynamic Risk Management and the Rise of Perpetual KYC

A significant shift underway across the region is the move towards dynamic, or “perpetual”, approaches to customer risk management. Traditional calendar-based periodic reviews are proving to be increasingly misaligned with the velocity of financial crime.

The research findings indicate that while many institutions remain reliant on static or reactive KYC models, a growing minority have begun to implement event-driven approaches that use continuous monitoring of internal and external data to trigger risk reassessment. Specifically, only 15.5% of institutions report having an advanced 'Perpetual KYC' model, while 39.5% operate a 'Hybrid Model' with automated triggers. This leaves 45% of institutions which are still relying on primarily static or reactive manual processes.

This transition represents a material change in how institutions conceptualise customer risk. Advanced toolsets increasingly enable continuous, lifecycle-based risk assessment - from onboarding through to ongoing monitoring - using customer and transaction behavioural signals. As risk decisions become more automated and event-driven, governance and operational complexity increase, particularly around data reliability, model explainability, and supervisory defensibility beyond traditional review cycles.

Maturity of Customer Risk Monitoring Models



Interview with Radish Singh
Asean Financial Services Risk Consulting Leader
EY

Radish Singh discusses the evolving financial crime landscape in the wake of major enforcement actions in Singapore, the critical shift from rule-based to model-based monitoring, and the often-overlooked importance of culture and conduct in AML risk management.

What are the most significant changes you have observed in the financial crime landscape over the last 12-18 months, and what are the key threats facing financial institutions today?

Radish Singh: The last 12 to 18 months in Singapore's financial crime landscape have been shaped by several high-profile money laundering investigations. However, while this brought significant attention, the underlying reality hasn't changed: the wealth management segment remains critical from an AML risk perspective. Singapore is a global hub for wealth management, attracting ultra-high-net-worth individuals, so the inherent risk is high. The cases reinforce the importance of robust, ongoing controls.

What is different now is the recognition that we cannot continue with existing methods. Banks involved will have to continuously enhance controls and monitoring. This means we need to use different techniques to monitor and manage risk, and assess the efficacy of our controls. We need to leverage technology, and slice and dice data and client profiles in a more targeted way. We need to move towards using models rather than rules to monitor risk. If we sharpen our approach to use technology to monitor and manage risk, we will be faster to react and be better able to weed out bad actors before they hit the books of the bank.

Beyond that, proliferation finance remains a key focus for Singapore, as does trade-based money laundering (TBML) and transaction monitoring. Interestingly, we also see the regulator very much focused on culture and conduct, and individual accountability, because they are all related.

What does this transition from rule-based to model-based risk monitoring entail and what are the benefits?

Radish Singh: The way transaction monitoring is done today is blunt and rule-based. You have set rules, scenarios and thresholds applied to each business segment. You might build some analytics or AI on top of that to triage or optimise it, but the foundation remains rigid.

Going model-based means we write models by learning from vast amounts of data – typologies, behaviours and anomalies we need to look out for. With rules, we are more deterministic, looking at a finite set of information. With models, you can be more probabilistic and cast the net wider. You can then reason that out with more features in the models to determine if something is truly an anomaly or a problem.

We are finding that institutions that have gone down this path are seeing two primary outcomes. First, the yield is higher, meaning they see more real anomalies that they didn't see with rule-based engines. Second is efficiency. Where there is noise, it gets suppressed because you don't want your resources focused on noise, which is what is happening today.

The empirical data suggests that the model-based approach is the way forward to better manage risk. We cannot allow our detection engines to continue to be straight-jacketed as we have been for all these years.

Beyond transaction monitoring, what are some of the most promising use cases for AI and generative AI in financial crime risk management?

Radish Singh: No conversation today is complete without talking about generative AI (GenAI). One of the clearest quick wins is in the wealth management space, specifically with source of wealth (SoW) assessment. This is a critical area of focus for regulators and a major

(Radish Singh interview continued)

pain point for banks. A lot of time spent onboarding ultra-high-net-worth clients is on understanding their SoW, their wealth journey, net worth plausibility and seed capital.

Using GenAI to perform SoW assessment is possible; the tools exist, and many banks are already creating their own. These tools can be configured to be fairly smart in how they synthesise data and highlight the risks within the documentation. This saves a lot of time and improves effectiveness because you can focus exactly where you need to.

Other use cases we are seeing include using GenAI for narrative generation when clearing alerts and, crucially, in automated alert adjudication. Today, much of the work to clear alerts from transaction monitoring or name screening systems relies on manual effort. An automated alert adjudication tool can do the work of a level one analyst in a very structured, systematic and standardised way. The output is then reviewed by a human, who can be far more objective because they aren't inundated with ploughing through noise.

Even with greater automation, you need humans in the loop for quality assurance and final assessment. For SoW, the final plausibility assessment must be done by a human.

What is the role of organisational culture in financial crime risk management, and what are the best practices for fostering a strong risk culture?

Radish Singh: Culture and conduct are possibly amongst the most difficult programmes to measure because they are intangible – focusing on behaviour and making decisions for the right reasons. They are key areas of focus for AML because of the conflicting priorities that can exist. For example, if a relationship manager's remuneration is driven by the assets they bring to the bank, it's likely they will do whatever it takes to get clients onboarded.

If you look at most financial crime or fraud cases, even with human oversight, decision-making can at times fall short. This highlights the limitations of relying solely on manual review. That's also where the regulator's concern comes from: how do we ensure decisions are made with the right risk lens and are consistent with the organisation's risk appetite?

> **"A good culture and conduct framework is not just about training. It needs to be embedded, starting with the 'tone from the top'. But we also need to look at the 'tone from the middle', because the issues are often in the implementation."**
>
> **Radish Singh, EY**

A good culture and conduct framework is not just about training. It needs to be embedded, starting with the "tone from the top". But we also need to look at the "tone from the middle", because the issues are often in the implementation. The programme must be able to pick up on conflicting priorities and allow people to make decisions without fear or favour.

This also means you need consequence management. Where there are behaviours that are not consistent with the risk appetite, these have to go through a consequence management framework with consistency to ensure there is a deterrence effect. The best programmes should also leverage behavioural monitoring and analysis, though many organisations don't necessarily have the appetite for this.

Why is there sometimes a reluctance among banks to adopt behavioural monitoring, and how do you justify its use?

Radish Singh: It's a combination of factors, including data challenges as well as the approach being seen as intrusive or like policing. It's a delicate balance. However, increasingly we see it's becoming a need.

When we conduct forensic analysis after an event has occurred, we generally find telltale signs. For example, if a case is rejected as not acceptable, but then there is silence for a few months before the same case resurfaces with pristine quality information – this can suggest somebody is actually helping to orchestrate profile-building to pass the bank's compliance checks.

That's what we mean by behavioural analysis. We are not looking at policing good people. We are looking at monitoring behaviour where it is anomalous and suggests that someone needs to intervene to contain the risk before it becomes a systemic issue for the institution.

Focused AI Deployment, Not Experimentation

Interest in AI remains high, but priorities have shifted from broad experimentation towards governed, use-case-specific deployment. While 'Integrating AI / Machine Learning' is the top technology priority for 50.6% of institutions, the actual implementation rates are more modest. For transaction monitoring, for instance, only 46.7% of institutions have implemented or are currently implementing AI/ML solutions.

Institutions are increasingly selective, concentrating investment on areas where AI demonstrably improves speed, prioritisation, or insight rather than attempting wholesale replacement of rules-based controls.

Common priority use cases include alert triage, network analysis, anomaly detection, and investigative support. At the same time, concerns around explainability, regulatory defensibility, and operational risk are shaping investment decisions. As a result, institutions are allocating resources not only to model development but also to governance frameworks, documentation, and human oversight.

This disciplined approach is echoed by practitioners on the front lines. "The way we use generative AI is not as a decision-maker, but as a tool, or what I'd coin an 'executive assistant'," explains Milan Gigovic of ANZ, describing the bank's 'Ultron' tool. "It does all the manual, 'swivel chair' labour of going into different source systems... It has been a game-changer, allowing us to make quick, informed decisions and provision timely intelligence."

This reflects an emerging consensus: AI is becoming a prerequisite for operating at scale, but institutions are arriving there in different ways. While a small number of banks report deploying AI-only detection in specific use cases, many - including large global systemically important banks — remain focused on controlled pilots and joint development initiatives. Across both approaches, effectiveness appears to depend less on the presence of AI itself than on how well it is embedded within a coherent operating model and supported by disciplined governance.

Sanctions, Trade, and Cross-Border Exposure

Sanctions and trade-related risks have risen sharply on the priority agenda, driven by geopolitical developments and heightened supervisory scrutiny. Institutions are reassessing how these risks are monitored, governed, and escalated – particularly where they intersect with fraud, payments, and broader financial crime controls.

However, the Barometer highlights a persistent gap between recognition and capability. While many institutions identify sanctions and trade exposure as high risk, fewer have prioritised their integration into core monitoring and investigation workflows. In practice, this disconnect is often reflected in high false-positive alert volumes that continue to absorb investigative capacity and obscure genuinely connected risk across domains.

As one respondent noted, "Despite the heightened focus on sanctions and trade risk, high false-positive alert volumes are still being reported. Investigators are spending significant time working through noise, which makes it harder to identify and escalate cases where sanctions, trade activity, and laundering risk converge."

This imbalance represents a growing vulnerability in a threat environment where sanctions evasion, trade-based abuse, and money-laundering activity increasingly co-occur — and where effectiveness depends not only on risk recognition, but on the ability to connect and prioritise signals across domains.

Collaboration: High Interest, Uneven Commitment

Collaboration and information sharing are widely cited as priorities, particularly in response to network-based crime. Yet commitment remains uneven. Legal uncertainty, data-sharing constraints, and unclear returns continue to limit participation in many markets.

"Information sharing has historically been a one-way street," said INTERPOL's Kang. "It needs to be a two-way street. Public authorities should share their data to help the private sector do their job better, especially since we are asking them to perform a police function by detecting crime."

Where collaboration is treated as infrastructure – supported by governance, technology, and senior sponsorship – it is increasingly viewed as a force multiplier. Where it remains ad hoc, its impact is marginal, with respondents noting that privacy and data-sharing regulations in many Asia-Pacific jurisdictions continue to limit how far collaboration can go. "The intent is there," one respondent observed, "but uncertainty around privacy obligations often acts as a handbrake."

As a consequence, commitment and impact remain uneven across markets. The Barometer suggests that collaboration is therefore likely to become a clearer differentiator of capability over the next cycle.

Organisational Change as the Hardest Priority

Perhaps the most challenging priority is organisational rather than technical. Converged risks require converged decision-making, yet many institutions continue to operate with fragmented ownership, budget structures, and accountability across fraud, AML, cyber, sanctions, and trade functions.

While technology and data initiatives dominate investment plans, fewer institutions report clear progress in redefining roles, bringing in new skillsets, escalation paths, and incentives across these domains. This misalignment continues to limit the impact of even well-executed technology programmes.

A Narrowing Window

The 2026 findings point to a narrowing window for adjustment. Institutions broadly agree on what needs to change, but execution remains uneven. Those that align priorities across technology, data, governance, and operating model are beginning to close the gap between risk and response. Others risk falling further behind as financial crime networks continue to adapt faster than institutional change.

In this environment, prioritisation itself has become a risk decision. The question is no longer whether institutions understand the challenge, but whether their choices reflect its urgency.

Interview with Doron Goldbarsht
Founder and Director, Financial Integrity Hub, and Associate Professor, Macquarie University

Dr Doron Goldbarsht discusses the impact of Australia's Tranche 2 reforms, the looming 'capacity crisis' facing the entire AML/CTF ecosystem, and fundamental questions that need to be asked about the adverse social and economic consequences emerging from illicit finance.

How has the financial crime landscape in Australia evolved over the last 12-18 months?

Doron Goldbarsht: The main change has been the long-awaited reform to regulate "Tranche 2" entities. For many years, the Financial Action Task Force (FATF) criticised Australia for not regulating designated non-financial businesses and professions (DNFBPs, aka Tranche 2 entities). After several consultations, the amendment to the AML/CTF Act was passed in November 2024. This is a huge reform that will, among other things, expand the number of regulated entities from about 18,000 to about 120,000.

This obviously impacts the newly covered DNFBPs – real estate professionals: agents, buyers' agents, and property developers involved in high-risk transactions; professional service providers: lawyers, conveyancers, and accountants who provide specific services (e.g. managing client funds, creating companies); trust and company service providers: entities that form, manage, or act as trustees/nominee directors; and dealers in precious metals and stones.

But it also impacts the existing Tranche 1 entities and the regulator, AUSTRAC. It's a big impact on the entire ecosystem of financial crime mitigation in Australia. For lawyers, who have pushed back for years, there is a significant impact on issues like legal professional privilege.

What is the biggest risk facing the financial industry?

Doron Goldbarsht: The biggest risk isn't a particular criminal threat, but capacity. Criminals will find a way to clear their money and enforcement agencies will find a way to chase them. Yet the true challenge rests elsewhere. Capacity, in my opinion, is going to be the main challenge.

It's not just about having the laws in the books; we also need to deliver. But who is going to do the work? There is a lack of people to do the compliance and the enforcement. For the new reporting entities, do they possess the knowledge required to recognise and report suspicious transactions? What is going to be the quality of these suspicious matter reports? A system reliant on reporting is only as strong as the understanding that informs it.

For AUSTRAC, they need the capacity to handle the influx of data to transform volume into insight through emerging technologies such as advanced analytics and artificial intelligence. Yet technology alone cannot resolve what is ultimately a matter of orientation.

It's more than ticking boxes; it requires a cultural shift to a risk-based approach where you truly understand your business. A checklist may create the comfort of apparent compliance, but without reflection it risks becoming little more than ritual. This is where we are going to see the challenge.

What have been the unintended consequences of the AML regime?

Doron Goldbarsht: We have all these costly obligations on reporting entities, but we also have unintended consequences. For example, a bank might decide it doesn't want to deal with crypto, so you exclude innovation.

When a bank chooses to withdraw from engaging with cryptocurrency, innovation itself may be quietly set aside. When certain geographic corridors are deemed too risky, entire communities can find themselves standing at the margins of the financial system. And when individuals cannot produce the forms of identification we have come to require, exclusion becomes not a policy objective, but a lived reality.

This invites a deeper reflection on balance. What, ultimately, are we gaining, and at what cost? For decades, the discourse on financial crime has invoked the familiar estimate that illicit financial flows account for roughly 2 to 5% of global GDP. This figure dates back more than 30 years, from work done at the IMF in the

(Doron Goldbarsht interview continued)

1980s. Is this because we don't know the true scale of the problem? Or is it because whatever we do, it's not really helpful?

At the Financial Integrity Hub, we are working on a 'harm index' to try and assess the real harm, because it's not just numbers. It's the impact on people – we are looking at the adverse social and economic consequences emerging from financial crime. You can only tell whether the regime is effective, and know how to allocate resources, if you know the harms that you're balancing against.

Besides the Tranche 2 reforms, what other regulatory or legal developments are you watching closely in Australia?

Doron Goldbarsht: The question of director liability is very interesting. Currently, there is a case pending where ASIC, the corporate regulator, has filed a statement of claim against the directors and senior management of Star Casino personally. They are using a 'stepping stone doctrine', arguing that by breaching the AML/CTF Act, the directors breached their duty of care under the Corporations Act.

This is significant because when a bank is ordered to pay a substantial fine, the burden does not rest on an abstract corporate entity. It is carried, in no small measure, by shareholders – often the public, through their superannuation. This reality invites a reconsideration of responsibility.

Direct liability has the potential to sharpen attention at the highest levels, and this is what ASIC is pursuing. The outcome of the case could have far-reaching impacts on the entire industry. What follows, therefore, is more than litigation – it is a moment of jurisprudential possibility.

The judgment in this case, would extend well beyond a single case. It would signal a cultural evolution in governance, one that recognises that integrity within financial institutions is ultimately sustained not only by frameworks and controls, but by the ethical attentiveness of those entrusted to lead.

Where do you see the next frontier for collaboration and information sharing in fighting financial crime?

Doron Goldbarsht: Australia was one of the first countries to introduce public-private information sharing through the Fintel Alliance, and it has been very successful. But the new frontier is private-to-private information sharing.

If a bank knows about suspicious behaviour, instead of just reporting it to the regulator, they should be able to share it with other banks. Currently, the regulator only sees pieces of the puzzle, but if the private sector can share information amongst themselves, we can ensure the regulator gets a fuller picture.

It sounds simple, but it raises concerns that are both operational and philosophical. Who should serve as the custodian of such a platform? Should participation arise from mandate or from mutual recognition of collective responsibility? How do we preserve the delicate balance between security and privacy, between collaboration and the safeguards of competition law? Different jurisdictions like the US, the Netherlands, Singapore and Hong Kong have different approaches to this.

The recent reforms in Australia have made it a bit simpler to share information by amending the tipping-off offence, but there is still no formal process or procedure in place. It's not a 'thing' yet, but these discussions are important, and the Financial Integrity Hub is engaging with these questions, noting that the future is often shaped long before policies are written.

What is the role of new technologies like AI in AML/CTF compliance?

Doron Goldbarsht: We should adopt AI, but we need to be cautious. I see it as only another layer of protection; it cannot replace human review. We need to understand its weaknesses.

In an era where saying "AI" has become almost obligatory in the language of innovation, there is a risk that enthusiasm may outpace reflection. Technology should not be embraced simply because it is new, but because it is understood.

The same goes for how we treat other technologies like virtual assets; there are still many regulatory questions to address around these new products and service providers. And so the task before us is not merely adoption, but stewardship: to ensure that technological progress advances financial integrity rather than quietly eroding it.

Substance Over Form: Evolving Regulatory Expectations

Regulatory expectations across Asia-Pacific are evolving less through incremental rule-making than through accumulated supervisory experience. A succession of high-profile investigations and enforcement actions in recent years – many involving cross-border payments, large-scale scam activity, and complex laundering networks – has exposed a recurring pattern. Institutions that appeared compliant on paper often proved less effective in practice.

The latest round of FATF mutual evaluations has reinforced the same conclusion, accelerating a shift in supervisory emphasis from form to substance. While formal requirements continue to differ by jurisdiction, the trend is increasingly consistent: institutions are no longer assessed primarily on whether controls exist, but on whether they operate effectively under real-world conditions.

Effectiveness as a Supervisory Standard

Across the region, supervisors are signalling that effectiveness is becoming the primary lens through which compliance frameworks are judged. This includes the capacity to detect emerging risk early, connect activity across domains, and escalate coherently in time to disrupt illicit activity – if not in real-time.

Measures that once signalled robustness – alert volumes, system coverage, or policy completeness – are increasingly secondary to questions about decision-making quality, investigative depth, and end-to-end outcomes. Recent enforcement actions and evaluation findings have sharpened this focus. Institutions that struggle to explain how their controls mitigate contemporary threat patterns face heightened scrutiny, even where formal requirements are technically met.

In this context, fragmented systems and siloed ownership are no longer viewed as neutral organisational choices. They are increasingly treated as structural weaknesses that inhibit effective risk management.

Data Quality, Lineage, and Accountability

Data has emerged as a central supervisory concern, shaped directly by lessons drawn from investigations and evaluations. In several recent cases, control failures were traced not to the absence of monitoring systems, but to inconsistent data, weak lineage, and an inability to assemble information across systems quickly enough to identify connected activity.

As a result, regulators are placing greater emphasis on data quality, consistency, and accountability – particularly where advanced analytics and AI support risk decisions. Institutions are increasingly expected to demonstrate not only what decisions are made, but how they are made: which data is used, how it is transformed, and who is accountable for outcomes.

Weaknesses in data governance now translate directly into questions about management oversight and control effectiveness.

AI and Model Governance

The same experience is shaping supervisory attitudes towards AI. Regulators broadly recognise that advanced analytics are necessary to manage scale and speed, particularly in high-volume payment and scam-driven environments. At the same time, enforcement outcomes and mutual evaluations have reinforced scepticism towards opaque models that cannot be explained, challenged, or governed.

The 2026 findings suggest that institutions deploying AI without clear documentation, validation, and escalation frameworks face growing regulatory risk. Conversely, those able to articulate model logic, monitor performance, and demonstrate responsible use are encountering greater supervisory tolerance – even where outcomes remain imperfect. The message is increasingly consistent: innovation is acceptable; opacity is not.

Expectations of Collaboration and Information Sharing

Investigations into large-scale, network-based activity have also shaped supervisory expectations around collaboration. While formal mandates for information sharing remain limited, supervisors are increasingly supportive of structured initiatives that demonstrably improve detection and disruption – particularly where risk spans institutions or jurisdictions.

The Barometer suggests that regulators view well-governed collaboration as a marker of institutional maturity, especially where it enables earlier identification of cross-institutional or cross-border risk. At the same time, supervisory tolerance remains closely tied to governance, legal basis, and accountability. Participation alone is insufficient. Institutions are expected to demonstrate how shared intelligence informs decisions, accelerates response, and improves outcomes – despite legal and operational frictions that will continue to constrain progress unevenly across jurisdictions.

Some industry leaders believe the impetus for deeper collaboration must come from the top. "Ultimately, I believe it has to come from the government to drive an economic crime strategy," argues Milan Gigovic of ANZ. "I would love for the government to mandate this collaborative approach... We need the courage from leadership across government and industry to come together and say, 'We have to do this, and we have to do it now'."

Supervisory Convergence, Local Execution

FATF mutual evaluations are contributing to greater convergence in supervisory expectations at a regional level, even as execution remains jurisdiction-specific. Institutions operating across multiple markets are increasingly required to navigate this dual reality: aligning internal frameworks with evolving international standards while responding to local supervisory priorities shaped by domestic enforcement experience.

The 2026 findings highlight the growing importance of internal consistency. Institutions with fragmented regional implementations struggle to demonstrate effectiveness, even where individual country programmes appear compliant in isolation.

A Narrowing Margin for Explanation

Taken together, recent enforcement actions, mutual evaluations, and supervisory engagement point to a narrowing margin for explanation and remediation. Regulators are increasingly unwilling to accept persistent weaknesses attributed to complexity, legacy systems, or organisational structure.

In this environment, the burden of proof is shifting. Institutions are expected to demonstrate that their compliance frameworks are proportionate, integrated, and effective against contemporary threats. The question supervisors are now asking is no longer whether controls exist, but whether they work.

Implications and Outlook

Effectiveness as the Defining Test

The 2026 Barometer captures the industry at a point of transition. Financial crime risk across Asia-Pacific is now faster, more networked, and tightly integrated across fraud, AML, cyber, sanctions, and trade. At the same time, the tools available to institutions have never been more capable. The gap that now matters most is no longer technological, but organisational and operational – a pattern observed consistently across survey data and supervisory interviews rather than in isolated cases.

Across the region, institutions broadly recognise the nature of the challenge. Risk is converged, data-driven, and adaptive. Responses, however, remain uneven. A small number of institutions are beginning to align technology, data, governance, and operating models around this reality. Many others continue to rely on architectures and decision-making structures designed for a more linear, fragmented risk landscape – one that no longer exists.

The Barometer's findings point to a decisive shift in how capability is judged. Investment in technology is no longer a proxy for resilience. Regulators, boards, and senior management are increasingly focused on outcomes: the ability to detect risk early, connect signals across domains, and intervene with speed and confidence. In this environment, fragmentation – whether technical, organisational, or informational – has emerged as a primary source of exposure. Partial convergence – modern tools layered onto fragmented decision-making – has become one of the most persistent causes of supervisory disappointment.

Data quality and integration stand out as the most consistent differentiators of effectiveness. Advanced analytics and AI can materially improve detection and prioritisation, but only where they rest on coherent data foundations and disciplined governance. Institutions that treat AI as a capability to be orchestrated, rather than a solution to be deployed, are better positioned to adapt as threats evolve and supervisory expectations continue to tighten.

The implications extend well beyond technology or planned investment programmes. Converged risk demands converged accountability. Organisational boundaries that once mirrored regulatory categories increasingly impede timely decision-making and effective response. Addressing this challenge requires sustained leadership attention and a willingness to revisit long-standing assumptions about ownership, escalation, and performance measurement. As expectations evolve, accountability is moving higher within organisations, with boards and senior management increasingly judged on outcomes rather than assurances.

The path forward is increasingly clear. Fraud and financia crime risk will continue to evolve in ways that test speed, coordination, and judgment. Supervisory scrutiny will continue to favour demonstrable effectiveness over formal compliance. Collaboration, data sharing, and

cross-domain intelligence will become more central, not less, despite the legal and operational frictions involved. In many institutions, the speed of decision-making and escalation remains mismatched with the velocity of risk.

The question facing institutions is no longer whether change is required, but whether it is occurring at the pace the environment demands. If risk now moves in days or minutes, can frameworks that adapt over years remain credible? The 2026 AML Tech Barometer suggests that while progress is evident, the margin for delay is narrowing. Effectiveness – measured in outcomes, not intent, investment, or architecture – has become the standard by which AML compliance frameworks will be judged.

This paper was published by Regulation Asia in collaboration with NICE Actimize.

About NICE Actimize

As a global leader in artificial intelligence, platform services and cloud solutions, NICE Actimize excels in preventing fraud, detecting financial crime and supporting regulatory compliance. Over 1,000 organizations across more than 70 countries trust NICE Actimize to protect their institutions and safeguard assets throughout the entire customer lifecycle. With NICE Actimize, customers gain deeper insights and mitigate risks.

Learn more at www.niceactimize.com @NICE_Actimize

Get in touch

Matthew Field
APAC Market Lead for Anti Money Laundering
NICE Actimize
Matthew.Field@niceactimize.com

About Regulation Asia

Regulation Asia is the leading source for actionable regulatory intelligence for APAC markets. Through our news, events, and research, we serve over 30,000 financial services professionals from more than 1,000 financial institutions, as well as regulatory bodies, exchanges, technology firms and other service providers.

www.regulationasia.com @RegulationAsia

Get in touch

Bradley Maclean
Co-Founder
Regulation Asia
brad.maclean@regulationasia.com

© Copyright 2025 Actimize Inc. All rights reserved.