

A 1LoD Report



# The Financial Crime Summit

NEW YORK

27 | Feb | 2025

FORECAST 2025

## Towards Intelligence-led Financial Crime Compliance: Reframing Risk for a Changing World

### Lead Sponsors



**QUANTIFIND**  
THE RISK INTELLIGENCE COMPANY



**SymphonyAI**

### Associate Sponsors

accenture

Davies

DOW JONES  
RISK &  
COMPLIANCE

eClerx®

encompass

feedzai

Guidehouse  
outwit.complys™

KPMG

MOODY'S

NAPIER

NICE  
Actimize

RIPJAR

### Exhibitors

ALLOY

Flagright

Greenlite

HERE

Hummingbird

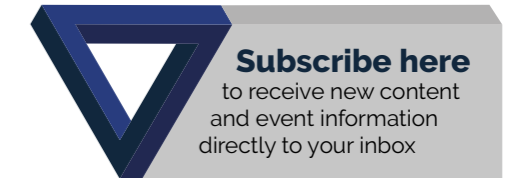
quantexa

saifr

SAYARI

sigma360

# Key Takeaways



## The technology gap is structural, not just technical

Despite advances in Artificial Intelligence (AI) and analytics, most financial institutions are constrained by legacy systems, poor data, and a bureaucratic compliance culture. If these simple basics are not fixed, new tools will probably be applied superficially rather than strategically.

## AI must serve as a support tool, not a silver bullet

AI is best used for automating low-value tasks and prioritising alerts, but it cannot replace human judgment. Explainability, oversight, and robust governance frameworks are essential for its safe and effective use.

## Culture and capability matter more than headcount

Adding more staff is not the answer. Institutions must invest in high-calibre talent with cross-functional expertise, such as analysts, technologists, and behavioural scientists who can drive change, rather than just executing tasks.

## Behaviour-based risk is the future of anti-money laundering (AML) and sanctions

Static, rules-based systems are no longer enough: Firms must adopt more dynamic, intelligence-led approaches to detect behavioural anomalies and assess client activity over time, rather than just checking against a list.

## Client Risk Rating (CRR) models must evolve into living frameworks

CRR models are too often static, outdated, and disconnected from real-world behaviour: They should incorporate feedback loops, behavioural insights, and ongoing calibration to be more effective.

## Compliance must shift from defence to design

The future of financial crime compliance lies in early integration, agile thinking, and strategic ownership. Functions must move upstream, influencing product design, client strategy, and enterprise risk, rather than responding after the fact.

## Screening of adverse media is underused

Adverse media screening can flag risks long before the transactional data comes in, yet this information is kept separate from other monitoring functions. Integration with transaction monitoring and onboarding can provide a more complete 360-degree view of the risks.

## Sanctions risk management has entered a new phase

With geopolitical volatility and complex forms of evasion on the rise, sanctions compliance must evolve beyond list-based screening to provide holistic surveillance of networks, jurisdictions, and transaction patterns.

## Fraud risk must be treated as strategic, not operational

Institutions need to shift from reactive fraud controls to proactive, business-integrated strategies. This includes better scenario planning, clearer ownership, and the use of behavioural intelligence across the client lifecycle.

## De-Risking is no longer just regulatory, but commercial

Institutions are increasingly getting rid of clients not because of the inherent risk, but because of cost and operational complexity. This raises concerns about financial exclusion and systemic blind spots.

# Towards Intelligence-led Financial Crime Compliance: Reframing Risk for a Changing World

**1LoD's Financial Crime Summit – New York 2025** brought together leading practitioners in the North American fight against financial crime: more than 350 people gathered for the one-day Summit, to explore all elements of financial crime risk management and hear the views of the industry's top executives.



**Subscribe here**  
to receive new content  
and event information  
directly to your inbox

### Confronting the Gap Between Potential and Practice

The event opened with a sharp critique of the status quo in financial crime compliance. Despite AI's great potential, particularly in transaction monitoring, sanctions screening, and know your customer (KYC), most financial institutions remain bound to legacy systems and outdated workflows. As one speaker put it bluntly, "We're still talking about the same big process flows," highlighting a widespread organisational reluctance to re-engineer basic elements such as data governance, investigative integrity, and contract structures.

Panellists warned that inefficiencies would become more entrenched if firms use a superficial overlay of AI tools without fixing the underlying architecture. AI, particularly large language models (LLMs), is treated as a tool for triage and acceleration, and not for decision-making. Participants stressed the need for explainability, model governance, and regulatory alignment. One speaker captured the regulators' evolving stance, saying, "Provided it's explainable, controlled and documented, regulators are starting to support this shift."

Rules-based detection systems were subjected to scrutiny. Panellists agreed that legacy rules are ill-equipped to detect behavioural anomalies or emerging threats. Yet firms which have invested in analytics and typology development find that their insights often fail to reach the onboarding process or monitoring systems. "This intelligence is rarely applied outside of investigations," one speaker said, citing a widespread inability to connect tactical learning to strategic design.

Participants discussed the growing friction between global consistency and regional regulatory nuance. Differences in definitions of beneficial ownership, customer risk, and documentation standards prevent firms from being consistent worldwide. Panellists stressed the need for collaborative dialogue with regulators to achieve greater harmonisation without sacrificing local relevance.

### People First, But not People Only

The final plenary tackled a core issue: while technology is evolving rapidly, its effectiveness depends on human understanding, integration, and accountability. "You can't really develop good

capabilities unless you know what you're trying to build for," said one panellist, stressing that context and clarity are prerequisites for meaningful innovation.

Panellists resisted the idea that technology alone could future-proof financial crime programmes. Instead, they wanted to see targeted resourcing, with fewer but more capable individuals who can drive change in the system. As one panellist explained: "It's not the number of people, it's who they are – and if they have a seat at the table."

Attendees were cautiously optimistic about integrating tech: While innovation in analytics and monitoring was acknowledged, implementation challenges – such as those related to data fragmentation and integration friction – remain acute. "It's not the tech that's the problem – it's the data that feeds it," said one speaker. Parallel running, model validation, and training requirements add to the operational burden.

A strong case was made for changing the culture of compliance, from one of tactical firefighting to one of long-term capability building, where financial crimes compliance (FCC) moves upstream so it is involved in the development of products at a much earlier stage. As one contributor put it: "If it takes 18 months to tune your system, you're already exposed."

The guiding principle must be agility, not just in responding to regulatory change, but in anticipating new types of financial crime and reshaping systems accordingly.

***"The Financial Crime Summit brought together industry thought leaders and practitioners across banking, fintech and crypto who shared valuable insight into fincrime themes and focus areas."***

CJ RINALDI, CHIEF COMPLIANCE OFFICER, KRAKEN

The Financial  
Crime Summit -  
New York 2025  
at a glance:



356  
Attendees



4  
Regulators



23  
Sponsors



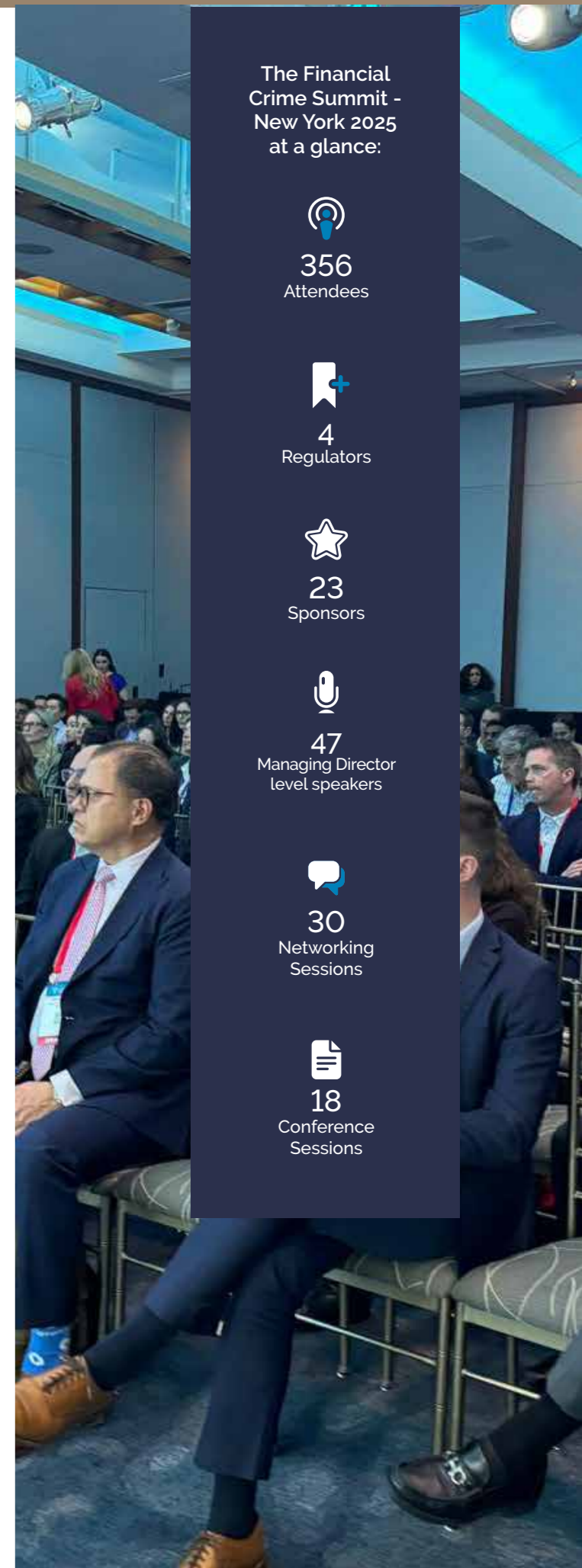
47  
Managing Director  
level speakers



30  
Networking  
Sessions



18  
Conference  
Sessions





### Anthony Scaramucci: Leadership and the Ethics of Risk

Anthony Scaramucci's closing speech was a powerful counterpoint to the day's technical discussions. With characteristic candour, he reflected on his journey from modest beginnings in Long Island to success on Wall Street, political humiliation, and ultimately, personal recalibration.

Scaramucci's narrative was both cautionary and redemptive. His brief but infamous tenure as White House Communications Director – cut short after just 11 days – was described as a turning point: "It sucked in a way you couldn't possibly imagine," he said, later adding, "You may not be okay in that moment, but you've got to trust yourself that you're going to be okay."

His key message was clear: ambition without self-awareness is dangerous. Accepting such a high-profile political role despite his own ethical misgivings – and against his wife's advice – was an ego-driven decision which had painful consequences. "That was one of the worst decisions I've made."

Scaramucci criticised the dysfunction he observed in the Trump administration, noting the paralysis it caused across government: "They're immobilised because they don't want to get fired or tweeted at." He linked this chaos to institutional stagnation, including in regulatory spheres that affect finance and crypto.

He emphasised the importance of culture and leadership in compliance, and why integrity matters in the commercial world: "The biggest risk is people. You can smell it on someone when they're willing to go over the line...I don't even have a personal trading account. My name is my currency."

Despite the levity and unscripted delivery, Scaramucci's message carried weight: Ethical leadership and strong governance are not luxuries, but are critical for institutions navigating uncertainty and complexity.

### AML & KYC: Rebuilding Foundations, Not Just Tools

The areas of AML and KYC are still defined by structural fragmentation and uneven maturity. While innovation is under way, particularly in relation to automation and AI, foundational problems persist: data is poorly structured or siloed, systems don't speak to one another, and processes are built on a periodic review logic that often ignores behavioural risk.

Panel discussions returned repeatedly to the limitations of current transaction monitoring frameworks. Despite regulatory scrutiny and major investment, institutions are failing at the basics. Panellists cited recent enforcement actions where more than 90% of transactional activity had not been monitored appropriately. Compounding this, new products are often launched without corresponding updates to detection logic, highlighting the disconnect between innovation and control. While some institutions are adopting layered detection models that combine rules-based triggers with machine learning and human review, this is the exception rather than the norm.

Screening for adverse media is also underused. Several panellists shared examples of situations where reputational red flags appeared months before any transactional anomalies. Yet these tools often operate in isolation, with few banks achieving the kind of integrated intelligence needed for a full risk profile. The gap, as one speaker described it, is not in technology but in application: "This isn't a tool problem, it's a data and design problem."

The discussion about client risk rating models underscored this diagnosis. While CRR systems are central to how firms allocate resources and manage due diligence, they are often outdated, generic, and poorly connected to real-world behaviour. Many models still overweight static factors such as customer type or jurisdiction – approaches that misallocate resources and increase operational friction. As one panellist put it: "We're good at bolting on new risks, but poor at de-risking outdated factors."

Participants agreed that CRR must be treated as a living framework – one shaped by behavioural intelligence, supported by feedback loops, and continuously recalibrated. Yet this evolution is often hampered by poor data and a lack of front-office engagement. Many institutions lack the governance structures to integrate insights from transaction monitoring or overrides from suspicious activity reports back into their risk models.

Another pressure point is bringing new customers on board. Despite widespread calls for standardisation, most firms continue to rely on fragmented, jurisdiction-specific processes that undermine efficiency and client experience. Panellists said they want a more centralised KYC framework supported by automation, smart document management, and better reuse of internal data. Yet they also warned against treating automation as a shortcut. Without a genuinely risk-based approach – one that considers real-time client behaviour – onboarding is a repapering exercise, not a strategic capability.

***"The Financial Crime Summit is an exceptional event that brings together the brightest minds in the industry. The caliber of speakers and delegates is unmatched, providing invaluable insights into the latest trends and challenges in financial crime prevention. The content is both comprehensive and actionable, and the networking opportunities are second to none. Attending this summit has been instrumental in enhancing strategies and building meaningful connections with industry leaders."***

OMER ASLAM, EXECUTIVE DIRECTOR- HEAD OF FINANCIAL CRIME COMPLIANCE ADVISORY FOR INVESTMENT BANKING, JP MORGAN



This information was taken from  
The Financial Crime Summit in  
New York, February 2025.

### Sanctions: From List-Based Filtering to Network-Based Detection

Sanctions compliance has undergone a profound transformation since 2022. Formerly a narrowly defined, reactive function, it has become a strategic risk priority, commanding attention at board level and driving significant investment. But this evolution has brought new complexity. Panellists described the increasing sophistication of sanctions evasion, ranging from indirect trans-shipment routes to opaque ownership structures, and warned that traditional list-based screening is no longer fit for purpose.

For example, Armenia's dramatic surge in exports to Russia illustrates the nature of the problem. "No economy grows that fast unless it's become a transit platform," one speaker observed, pointing to the use of third countries to bypass controls. This has pushed institutions to focus not just on sanctioned entities or jurisdictions, but on transactional behaviours, network relationships, and end-use patterns. In practice, this means blending sanctions, AML, and export controls into a single, investigative framework.

Technology plays a crucial role here. AI is used to detect threat typologies, identify risk indicators buried in unstructured data, and monitor payment

flows in real time. But as with AML, technology alone is not enough. The effectiveness of these systems depends on data quality, model governance, and human oversight. "AI can get it wrong at scale as easily as get it right at scale," one speaker warned.

Internal controls are evolving, but slowly. Many firms still rely on generic screening logic that fails to align with specific business activities. Speakers emphasised the need to embed controls directly into commercial processes, such as trade finance or foreign exchange, rather than treating sanctions as a stand-alone function. Data, again, emerged as the Achilles heel. Fragmented infrastructure and legacy systems make it difficult to achieve the completeness, timeliness, and traceability needed for effective sanctions management.

Training and culture are essential enablers of progress. Relationship managers don't need to become sanctions experts, but they must be able to recognise red flags and know when to escalate. One speaker summed up: "The goal isn't for a banker to know the law – it's for them to know when to pick up the phone."

***"1LoD brings together the leaders in Financial Crime Risk Management and the most innovative technology companies to combat crime."***

GRAHAM BAILEY, CHIEF OPERATIONS OFFICER, QUANTIFIND

### Fraud and Emerging Threats: From Silence to Strategy

Fraud is no longer only a concern for retail customers, but a strategic risk that cuts across private credit, digital assets, and traditional banking alike. Many institutions still approach fraud as an operational or reputational issue, rather than as a business risk that demands proactive management and strategic integration.

The rise of corporate loan fraud in the private credit sector is a key concern. Institutions described how fraudulent financial statements, fabricated contracts, and misrepresented litigation histories have become more common, requiring enhanced due diligence and forensic reviews far beyond AML baselines. At the same time, impersonation scams targeting executives and investors are increasing in frequency, often amplified by social media and messaging platforms.

Despite these challenges, frameworks to manage the risk of fraud are fragmented and often disconnected from enterprise-wide risk structures. Speakers said most fraud policies are too vague or too complex to be useful. Polling showed a lack of confidence in policy enforcement and a widespread view that responsibilities are poorly defined. "Fraud bad. Everyone responsible," one speaker quipped, satirising the ineffectiveness of generic mandates.

Cross-functional collaboration is essential. Fraud teams need to share intelligence with

AML functions, especially given the growing convergence of typologies. Behavioural data from fraud monitoring can support AML risk assessments, while financial crime teams bring deeper understanding of illicit typologies and regulatory expectations. The future lies in shared ownership of detection, response, and controls.

Emerging threats have led to renewed scrutiny of the risk-based approach, or RBA. While intended to allow proportionality and flexibility, the RBA is often misapplied, for example, when it is used as a rationale for reducing control rather than intelligent reallocation. Speakers warned that the RBA still needs to meet core regulatory expectations and document decisions rigorously. "Flexibility is not an excuse for failure," one participant said.

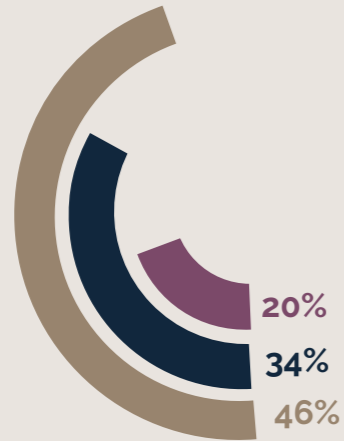
Discussions about de-risking were particularly charged: Institutions are increasingly walking away from clients not due to their inherent risk, but because the cost of compliance has become unsustainable. While some de-risking is commercially justified, speakers warned that it can push legitimate actors into less regulated spaces, exacerbating systemic risk rather than containing it.

If one theme unified the summit, it was the call for a deeper, more strategic form of compliance – one grounded in purpose, driven by intelligence, and built for change. The path forward is not about tools or templates. It is about clarity of intent, the courage to challenge legacy thinking, and the capability to build systems and teams fit for the future.

# Poll results

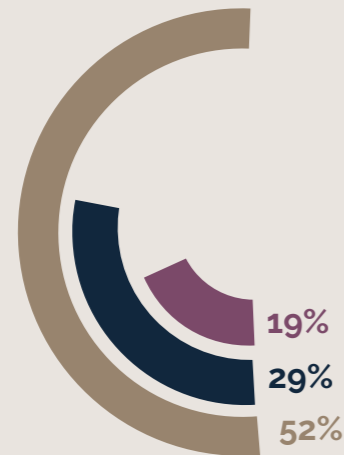
I believe that my organisation's financial crime function is fit-for-the-future:

- Yes
- No
- I don't know



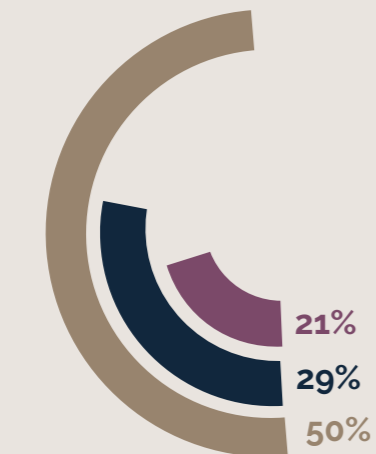
My expectation is that the complexity of the financial crime regulatory landscape is going to:

- Moderately increase
- Significantly increase
- Remain the same



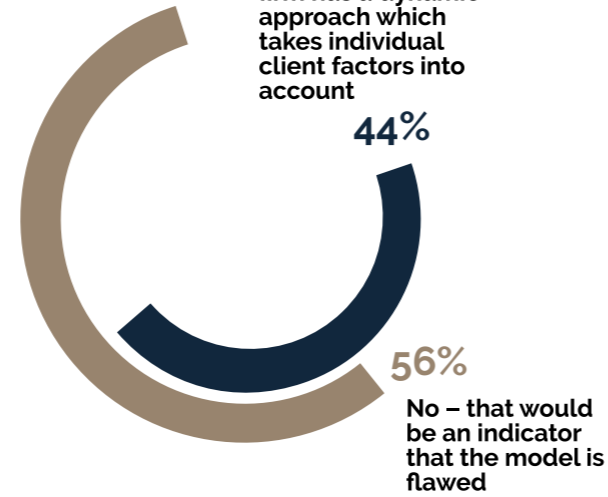
How involved is the front office in the review and challenge of your firm's client risk rating model? Choose one of:

- Somewhat – perhaps reluctantly, but they do play a role
- Very little – they largely leave it to the second line
- Very engaged – they are an important, indeed an integral, part of the review process

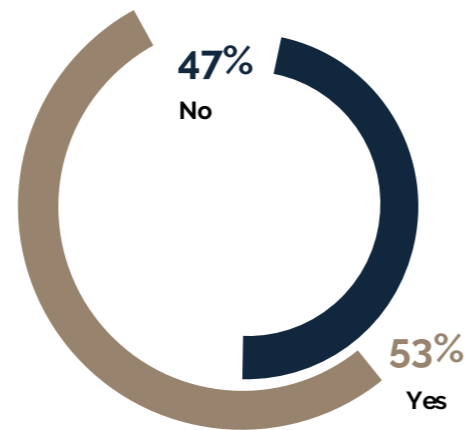


Risk rating over-rides: can an effective model have lots of risk rating over-rides?

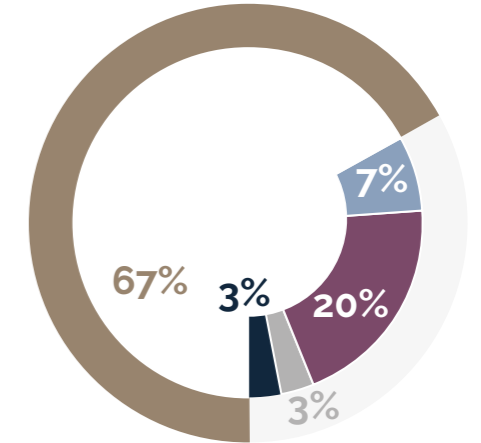
Yes – that shows the firm has a dynamic approach which takes individual client factors into account



Do you plan on accessing the FinCEN database this year?

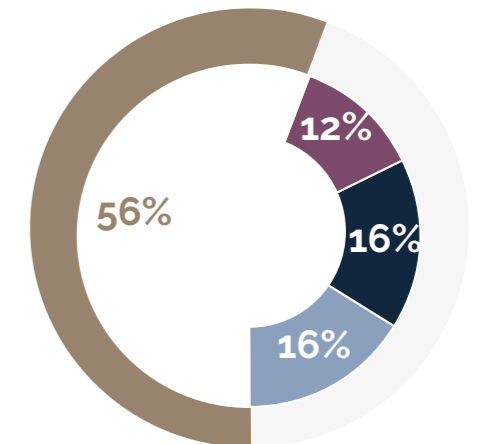


What do you see as the biggest challenge in enhancing transaction monitoring (TM) systems today?



- Data silos & integration issues – Lack of seamless connectivity between systems
- High false positive rates – Inefficiencies in current detection methods
- Legacy technology limitations – Outdated systems slowing down progress
- AI explainability & regulatory concerns – Black-box models and compliance hesitations
- Skills gap – Lack of AML professionals with technical expertise

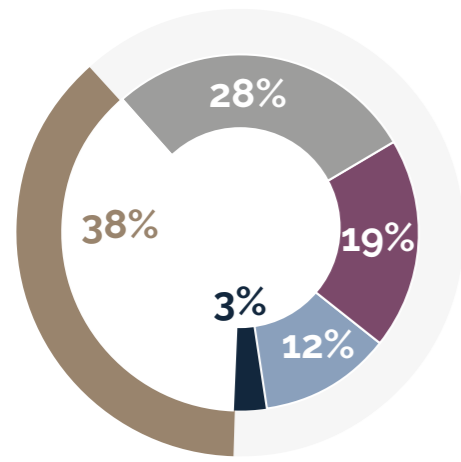
What is your organisation's current stance on AI adoption in transaction monitoring?



- Still rules-based, but exploring AI – Traditional monitoring with plans to adopt AI
- Experimenting with AI – Testing AI models but not fully implemented
- Minimal AI adoption – Heavy reliance on human-driven case management
- Actively using AI & machine learning – Fully integrated into our TM process

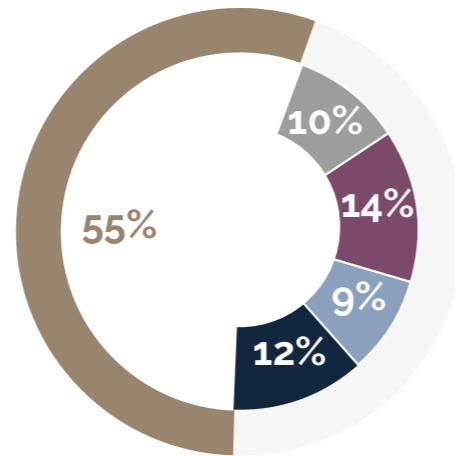
# Poll results

What is the most significant challenge facing the onboarding of clients?



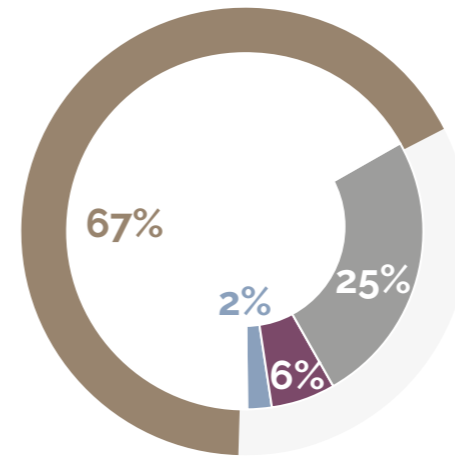
- Cumbersome and Time-Consuming Onboarding Processes
- Lack of Data Quality and Completeness
- Complex Client Structures
- Managing Internal Variations in KYC Requirements across Different Products and Business Lines
- Managing Variations in Jurisdictional Requirements

In which financial crime area is your firm prioritising the use of AI/machine learning/LLMs:



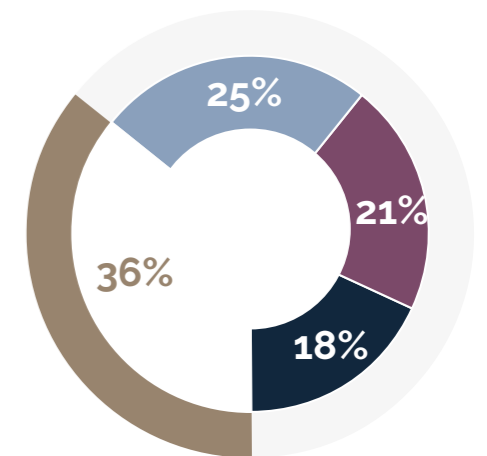
- Transaction monitoring
- Client on-boarding
- Something else
- Sanctions screening
- None – my firm is not using AI in the financial crime space

Do you believe that technology is advancing quickly enough to effectively combat and prevent financial crime? Choose one from:



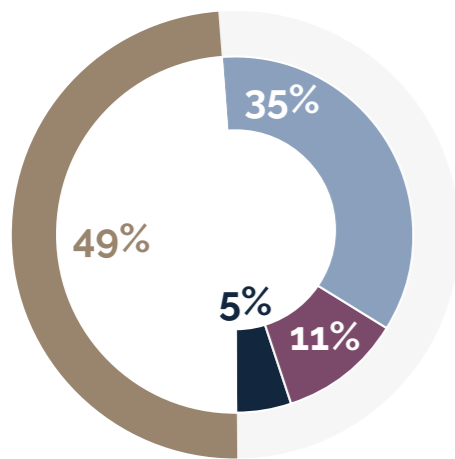
- Technology is advancing, but the challenge is how it's implemented by people
- No, the pace of technological advancement is not fast enough to stay ahead of financial crime
- Yes, technology is keeping up with financial crime
- Technology will never be enough as human expertise is critical in preventing financial crime

What is the primary benefit of using AI and machine learning in sanctions compliance?



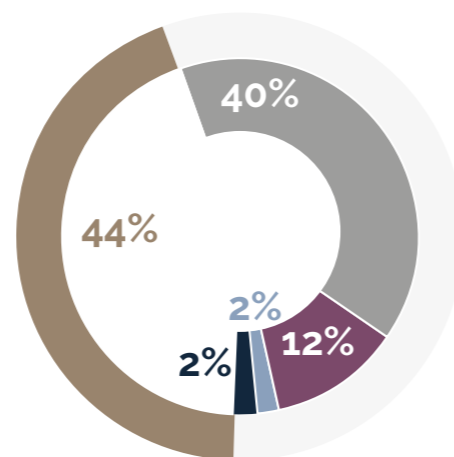
- AI is not widely used in our sanctions compliance program
- Faster response to evolving sanctions risks
- Increased accuracy in detecting suspicious transactions
- Combining alert feeds in screening and other functions

If my job depended on the effectiveness my firms' risk-based approach, I would sleep well at night?



- Agree
- Disagree
- Strongly Agree
- Are you having a laugh?

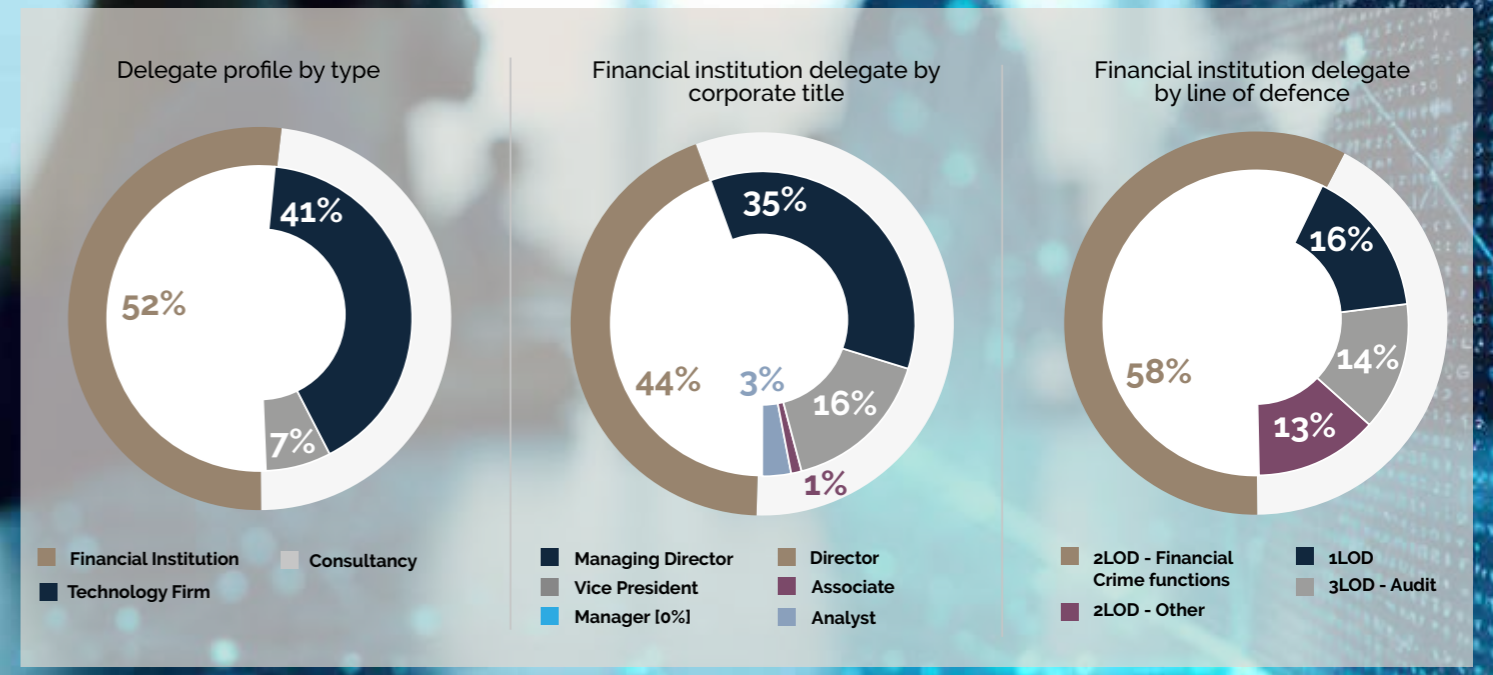
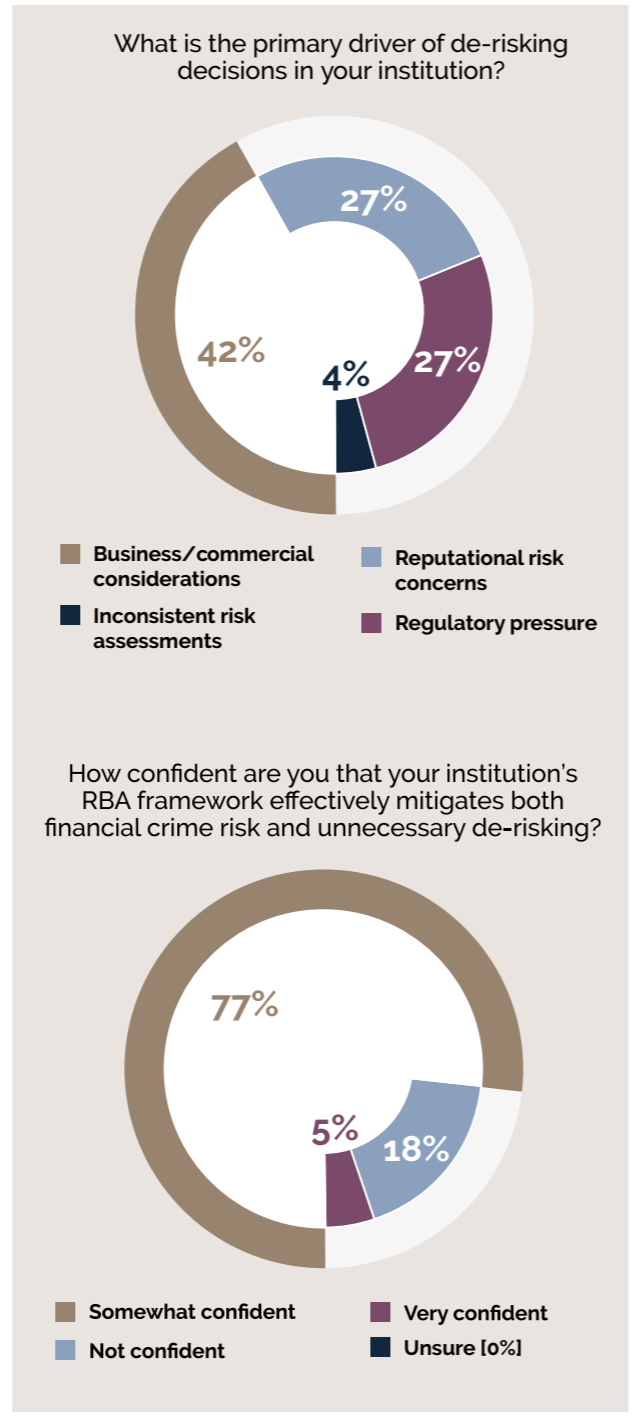
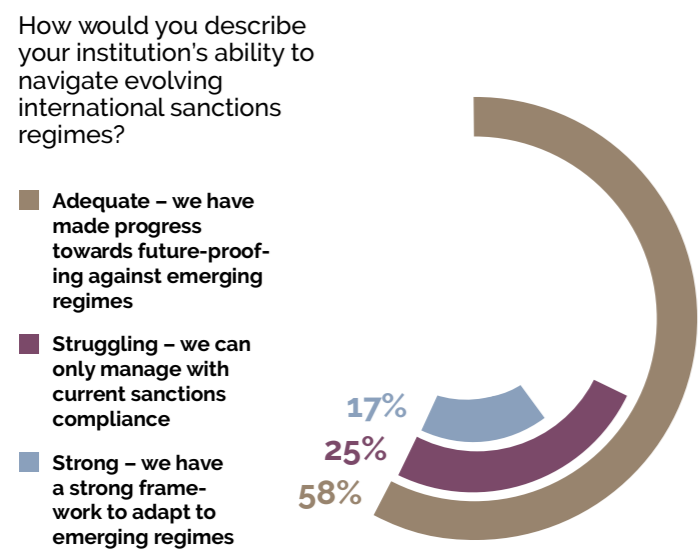
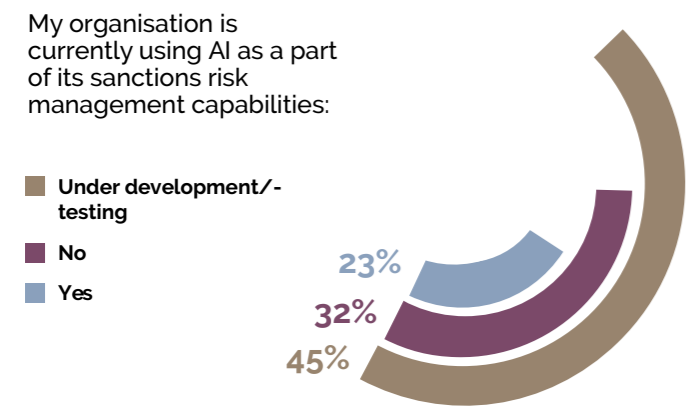
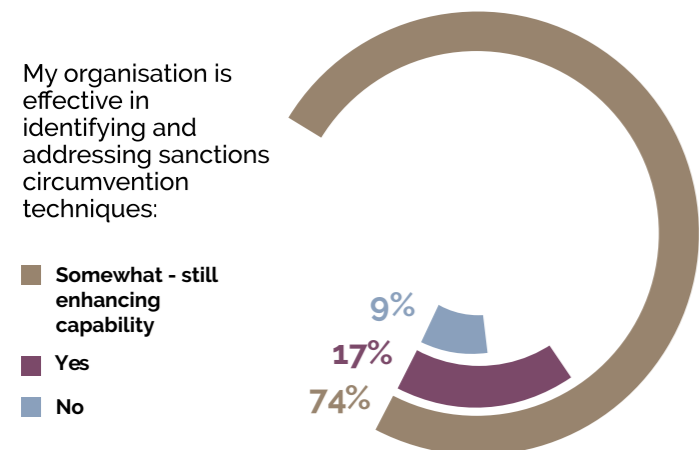
Looking across the banking sector, at what stage of evolution do you think firms have now reached in terms of tackling financial crime risks? Choose one from:



- Grown up but lacking worldly experience
- Adolescent
- Fully mature
- Toddler
- New-born baby



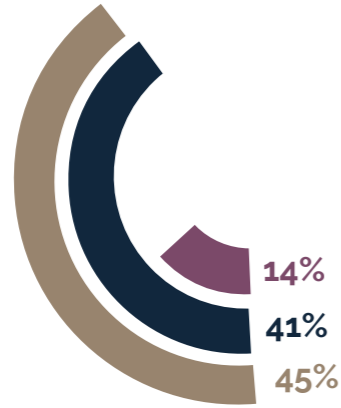
# Poll results



# Poll results

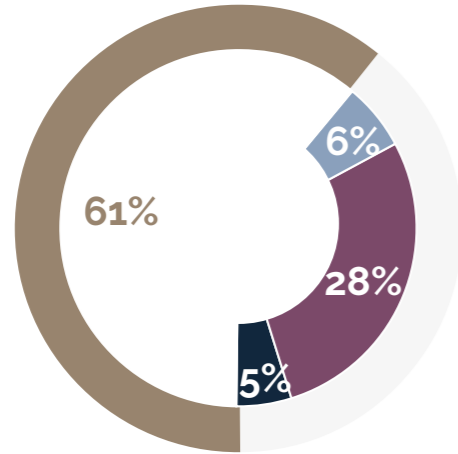
What is the biggest technological challenge in implementing fraud detection and prevention systems?

- High cost and resource constraints
- Data quality and integration issues
- Difficulty in adopting AI and machine learning at scale
- Regulatory and compliance barriers [0%]



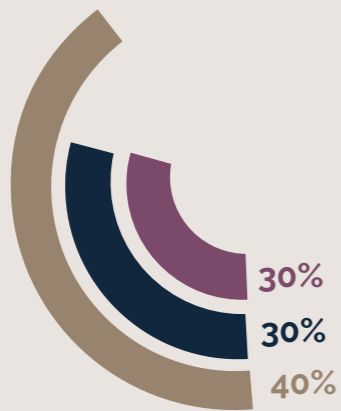
How effective do you believe current private-public collaboration is in combating fraud?

- Limited effectiveness – engagement exists but lacks impact
- Highly effective – strong cooperation and real-time intelligence sharing
- Moderately effective – some collaboration, but gaps remain
- Ineffective – minimal collaboration and slow response times

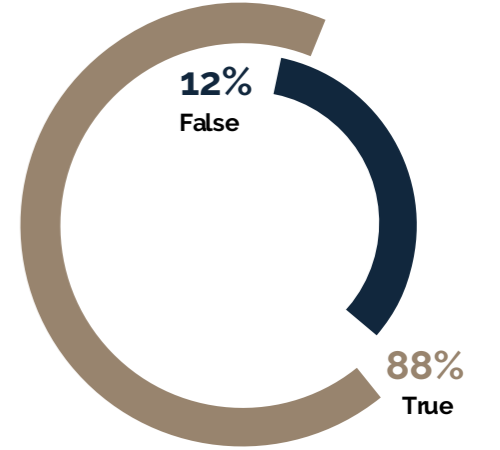


My organisation is currently providing services involving crypto and/or digital asset products:

- Evaluating/Exploring/Testing
- Yes
- No

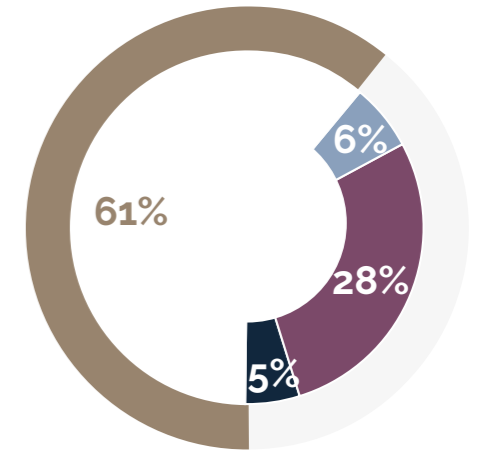


I believe US crypto and digital exchanges or platforms are subject to the US Bank Secrecy Act (BSA) and ALM legislation and regulation:



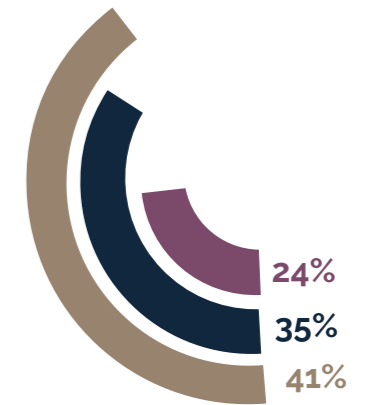
What tools are most effective in getting buy-in/support across the broader firm for a robust fraud risk management framework?

- Big fines from regulators
- Tabletop exercises
- Use industry intelligence to move the needle – to combat "it happens there but not here"
- Disciplinary actions for internal fraud



Which of these statements most closely reflects the position at your firm? Choose one from:

- We have a fraud policy - but the 1st line takes little notice and it is not enforced
- We have a fraud policy - and it's well-understood, embedded and effective
- We have a fraud policy - but no-one takes much notice of it, nor is it enforced
- We don't have a fraud policy [0%]



Upcoming Financial Crime events



2025

Responding to threats, redefining risk,  
rebuilding frameworks

IN-PERSON CONFERENCE

A 1LoD event



The Financial  
Crime Summit

LONDON

11 | Sep | 2025

VIRTUAL EVENTS

**01&02**  
July

Onboarding & KYC Deep Dive

**21&22**  
Oct

AML Deep Dive

**02&03**  
Dec

Fraud Risk Deep Dive

[www.1lod.com](http://www.1lod.com)