

Research Report

Untapped Potential

AI-enabled Financial Crime Compliance Transformation in Asia
Maturity, Applications & Trends

October 2024

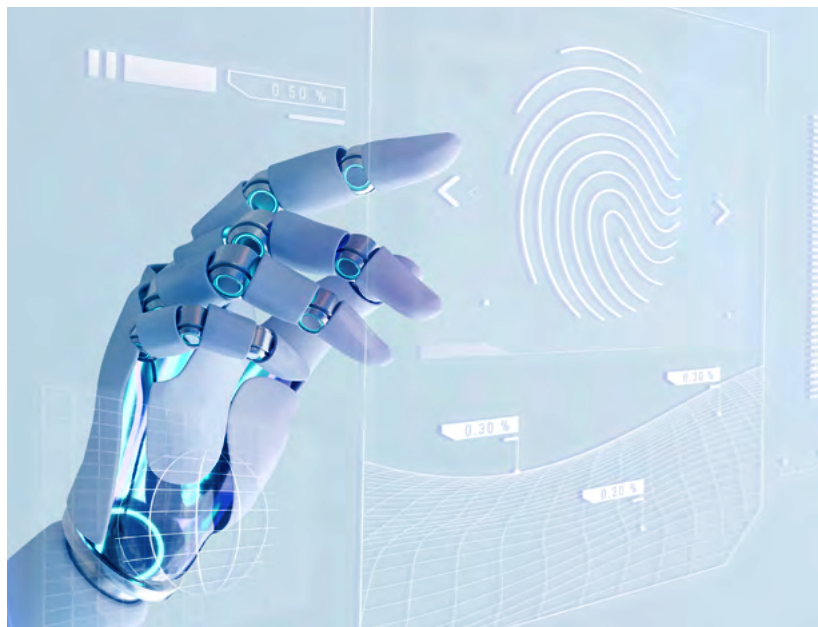
regulationasia.com



Contents

1. Executive Summary	3
2. Key Takeaways & Calls to Action	5
3. Introduction & Methodology	7
4. AI Deployment Maturity	9
5. Interview Box: Siddhant Sahai, Suncorp Bank	11
6. AI Deployment Strategies	14
7. Spotlight on GenAI: Opportunities & Risks	16
8. AI Adoption Challenges	18
9. Interview Box: Brent Estrella, Rizal Commercial Banking Corp	19
10. AI Value Articulation	22
11. Interview Box: Dr. Elea Wurth, Deloitte	24
12. Regional Regulatory Snapshot	27
13. SymphonyAI's Commitment to Responsible AI	30
14. Final Thoughts & Strategic Recommendations	31

I Executive Summary



“**Asia’s adoption of AI in financial crime risk management remains in its early stages.**”

In a world where financial crime continues to evolve at an unprecedented pace, financial institutions (FIs) must arm themselves with the most powerful tools to stay ahead. Enter Artificial Intelligence (AI)—technology that revolutionises the way financial services detect risk, manage risk, ensure compliance and stay ahead of criminals, costs, and community expectations. But as exciting as the potential may be, the reality on the ground tells a more complex story.

AI is not new to the financial industry; it has been deployed for a long time in areas such as algorithmic trading, fraud risk, credit scoring, and chatbots. However, the advent of Generative AI (GenAI)—which can create, enhance, summarise, and analyse unstructured data such as text,

code, and images—marks a new era, expanding the number of potential use cases.

The area of financial crime is a case in point, particularly money laundering, as it represents an escalating threat, accounting for up to 6.7% of global GDP and impacting a range of financial services businesses. In this regard, bad actors hold a significant advantage over FIs – due to their ability to adapt and evolve quickly. While complex structures and regulatory frameworks tend to encumber FIs, criminals are agile, rapidly adjusting their tactics to bypass safeguards.

Criminal actors are already embracing AI to exploit vulnerabilities present in outdated and less sophisticated compliance systems and controls. The rapid advancement of technology, paired with slower institutional responses, creates the perfect environment for organised crime to thrive. This is driving FIs to pursue a more effective and efficient response and better ways to automate processes and generate efficiencies, including by leveraging Predictive AI and GenAI, rather than continue with the longstanding and unsustainable industry strategy of throwing bodies at the problem.

Despite the growing interest in AI, our research shows that Asia’s adoption of AI in financial



One of the biggest impediments to FIs applying AI... is the challenge of integrating the technology into legacy systems.

crime risk management remains in its early stages. While GenAI continues to generate significant excitement, most FIs struggle to turn this interest into meaningful results. Rather, instead of delivering the expected improvements in efficiency and effectiveness, most FIs in the region remain focused on overcoming the complexities of traditional AI implementation. As a result, few have been able to fully leverage AI's potential to enhance risk detection and streamline compliance processes, leaving much of its transformative power untapped.

One of the biggest impediments to FIs applying AI in financial crime compliance processes, such as anti-money laundering (AML), is the challenge of integrating the

technology into legacy systems. Many firms find it difficult to justify the cost and complexity or to articulate the business case to their boards and senior management.

Data quality and availability are also seen as significant issues, as are data privacy and protection. Firms are starting to prioritise the use of AI to help them improve data quality, recognising that data is the lifeblood of a strong financial crime risk management programme, and the key to enabling other AI-related projects. Indeed, FIs often cite issues related to data quality, availability, reliability and integrity as the reasons that they are unable to more quickly progress their AI initiatives past pilot and experimental stages.

The lack of a harmonised approach in the regulatory landscape is yet another challenge that appears to be holding back AI initiatives. Firms have insufficient clarity on regulatory expectations and struggle to align their AI projects with existing rulesets, making them cautious about full adoption. Yet, it is widely recognised that the use of AI will be a key factor in creating a competitive advantage for first movers in the years ahead.

Still, the question is no longer around whether Predictive AI and GenAI will transform the financial crime compliance function, but how. As FIs face ever-increasing alert volumes, resource constraints, and constantly evolving regulations, adopting these technologies is quickly becoming an operational imperative. Predictive AI and GenAI offer the ability to process vast amounts of data in real time, improving efficiency and effectiveness by focusing resources on the highest-risk areas.

This not only enhances compliance but also reduces operational costs, minimises disruption to customer processes, and ultimately provides a competitive advantage by enabling FIs to focus on growth while managing risks more effectively. By moving quickly from proof of concept to full-scale production, early adopters can establish themselves as leaders in efficiency and innovation before these technologies become the industry norm.

FIs that seek to benefit from this first-mover advantage need to take a strategic approach to AI, including conducting assessments to determine the use cases that can generate the most value, adapting and updating their technologies infrastructure to take advantage of new innovations, and putting in place long term structures for governance, monitoring, evaluation and continuous improvement.

I Key Takeaways & Calls to Action

Key Takeaways from the Research:

1. Predictive AI and GenAI Adoption is in its Early Stages:

Despite the potential of Predictive AI and GenAI in financial crime compliance, most FIs in Asia remain in the early stages of deployment. Many firms still grapple with legacy system integration, data quality issues, and regulatory uncertainty.

2. Lack of Regulatory Clarity Continues to Hinder Adoption:

A lack of harmonised regulations and clear guidance from authorities, including around ethics and their application in domains like AI, is making FIs cautious about fully embracing AI. Banks struggle to align AI projects with existing compliance rules, slowing down adoption.

3. Operational Efficiency Brings a Focus on Risk:

Traditional methods of addressing financial crime are increasingly falling short in managing the speed and complexity of modern threats and allowing people the time to mitigate risk. Predictive AI and GenAI are increasingly seen as essential tools to enhance operational efficiency, AML effectiveness, and create the space for thinking and managing financial crime risk.

4. AI's Role in Data Quality Improvement:

AI technologies are being recognised for their ability to enhance data quality and governance. As FIs adopt AI, improving data management – the lifeblood of any financial crime programme – is seen as a key use case for the technology, and a crucial enabler for other AI-related projects.

5. Board and Executive Sponsorship is Key:

Senior executives and boards are seen as critical drivers of AI adoption. Strong leadership commitment and a proactive approach to regulatory engagement are considered essential to launch new AI projects, and ultimately advance them from proofs-of-concept to larger-scale implementations.

Calls to Action:

By acting on these key takeaways and calls to action, FIs can enhance their compliance programmes and ensure long-term resilience in a rapidly evolving financial crime landscape. The future belongs to those who proactively scale their AI capabilities, leverage technological advancements, and adapt to emerging risks.

1. Move beyond customer-facing functions and explore AI-based solutions for enhancing financial crime compliance capabilities.
2. Identify specific use cases where the positive impact from AI deployment is clear, such as false positive reduction, cost savings and efficiency gains.
3. Start with pilot projects and scalable implementations before gradually expanding AI's role within the compliance ecosystem.
4. Use recent financial crime incidents to demonstrate how AI can ensure more effective detection and prevention to help communicate clear value to boards and senior management.
5. Prioritise data governance to ensure high data quality standards are maintained, which is necessary to fully leverage AI technology.
6. Collaborate with regulatory bodies to gain clarity and guidance on AI deployment while ensuring compliance with evolving standards.



I Introduction & Methodology

“

FIs need to act swiftly to integrate technologies like Predictive AI and GenAI into their AML compliance and risk management frameworks.

The rapid digital transformation in financial services has not only opened new opportunities but also heightened risks, particularly in the area of financial crime. Bad actors have quickly adapted to the evolving landscape, continuously refining their tactics to exploit the digital environment – including by misusing AI for illicit activities. As these threats grow more sophisticated, financial services businesses must move beyond traditional defences and embrace advanced technologies like AI to stay ahead.

Recent financial crime cases across Asia illustrate the pressing need for FI

s to adopt Predictive AI and GenAI to detect and mitigate risks more swiftly and effectively. In Hong Kong, scammers used AI-driven deep fake video technology to impersonate senior executives during video calls, defrauding a multinational company of USD 25 million.

In Japan, during Interpol’s Operation HAECHI IV, authorities uncovered multiple cybercrime cases in which criminals utilised AI to bypass security measures in FI

s. The specific financial losses were not disclosed. Meanwhile in Australia, phishing scams powered by AI have become more prevalent. AI-enabled algorithms are being used to create highly convincing

phishing emails designed to deceive corporate executives and have led to millions in financial losses.

These examples illustrate the increasing sophistication of AI-based attacks, with criminals exploiting virtual communications, weak points in digital defences, and leveraging social engineering tactics to generate illicit proceeds from criminal activities. As these threats evolve with increasing speed, traditional compliance systems – hampered by slower response times and limited scalability – are no longer sufficient to keep up with their increasingly complex and adaptive nature.

GenAI in particular represents a powerful productivity frontier with the potential to add trillions of dollars in value across sectors, including approximately USD 200-300 billion for financial services. Its ability to contextually generate, analyse, and interpret vast amounts of unstructured data opens new avenues for improving operational efficiency, expanding financial crime risk coverage, and significantly enhancing detection and prevention efforts.

Time is of the essence, and FI

s need to act swiftly to integrate technologies like Predictive AI and GenAI into their AML compliance and risk management frameworks.

As regional and global regulators intensify their crackdown on financial crime, money laundering, terrorism financing, and sanctions evasion, it has become essential for FIs to adopt these technologies to strengthen their defences, ensure regulatory compliance, and remain competitive.

This research provides a comprehensive overview of the current state of AI deployment within FIs across Asia, with a

focus on adoption maturity, implementation challenges, and a review of the factors that enable AI projects, such as organisational readiness, technological capabilities, and regulatory support. It also examines how banks measure effectiveness and return on investment (ROI), as well as how the value of AI initiatives is communicated to internal and external stakeholders.

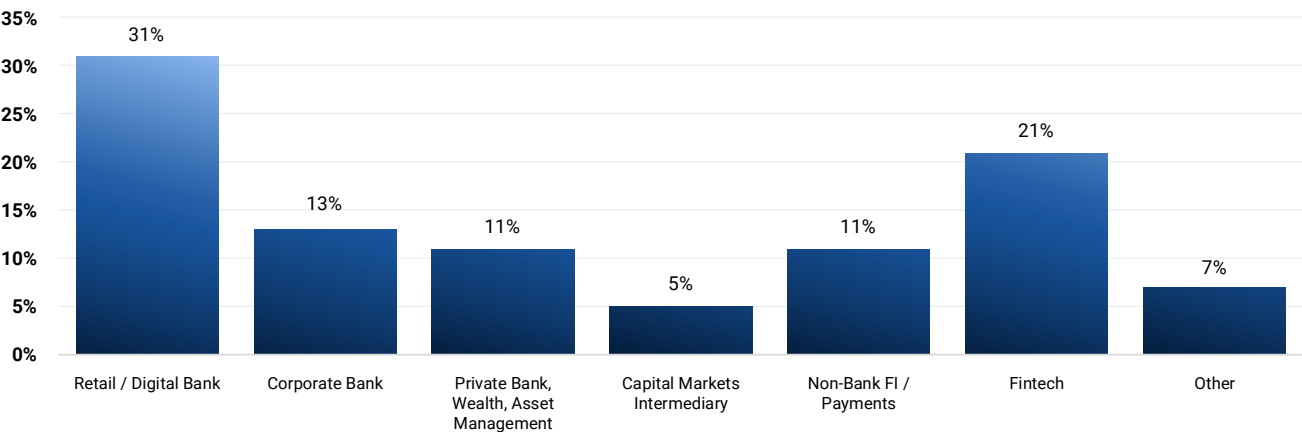
This report includes a dedicated section on GenAI, offering a view into current adoption trends, its potential use in financial crime prevention, and discussing some of the challenges FIs are experiencing in advancing these projects.

The findings presented in this report are based on data collected from surveys and interviews conducted with 126 financial crime compliance, operational and technology practitioners across Asia Pacific between July and September 2024.

The respondents represented a broad range of financial services businesses, including banking, wealth and asset management, capital markets, payments and other financial sectors. Almost two-thirds of respondents came from firms with assets under USD 10 billion; while about 20% of the respondents came from large global firms with over USD 100 billion in assets.

The majority of respondents were employed in risk, governance, financial crime compliance or technology roles, based in jurisdictions including Singapore, Australia, New Zealand, Malaysia, Philippines, Thailand, Vietnam, Indonesia, Hong Kong, and Japan, among others.

Type of Financial Institution



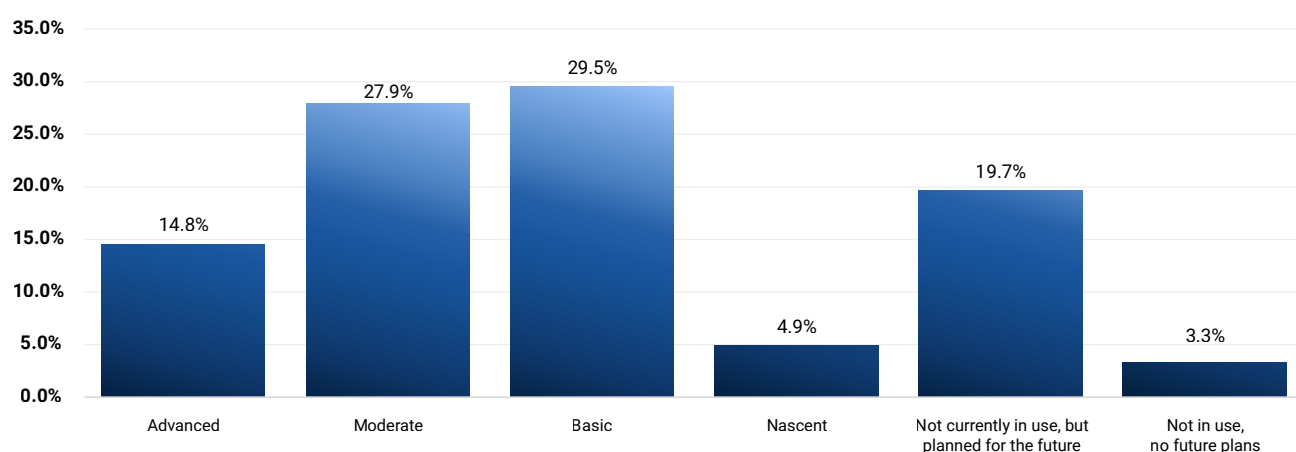
AI Deployment Maturity



Despite AI being a buzzword, the research found that its adoption and sophistication is still in early stages at most FIs. About 23% of respondents reported no use of AI within their organisations, while 34% assessed their sophistication in using the technology as “nascent” or “basic”. About 28% said they had “moderate” sophistication, while around 15% said they were at an “advanced” level of sophistication.

“The findings show a lower level of sophistication among FIs than was expected at this stage in the technology’s adoption curve,” said Bradley Maclean, Co-Founder and Head of Research at Regulation Asia. “Still, it is significant that only very few firms [3.3%] said they don’t have plans to deploy the technology in the future, indicating the wide recognition of its transformative potential.”

Sophistication of AI/ML Application in the Financial Institution



In AML-specific functions, deployment was also found to be lower than expected. Only a quarter of firms are actively applying the technology for AML, while another quarter are still in various stages of pilots. About 41% of respondents have yet to start on an AI adoption journey but have plans to do so in the future. A further 9.3% said they have no plans to implement AI in their AML functions.

The research found that global FIs were more likely to already be actively exploring the use of AI in AML-related initiatives compared to regional firms. Up to 55% of respondents from FIs with a global footprint said they were either actively applying AI or piloting the technology, compared to 28% of respondents at regionally-focused FIs. The vast majority of regional firms that were not already applying AI in AML-related functions said they plan to do so in future.

“There is still a strong preference for the traditional products that FIs already know, but we are seeing an increase in interest for AI-related products as the technology develops further and improves in sophistication,” said Craig Robertson, Financial Crime Subject Matter Expert - APAC, Financial Services at SymphonyAI.

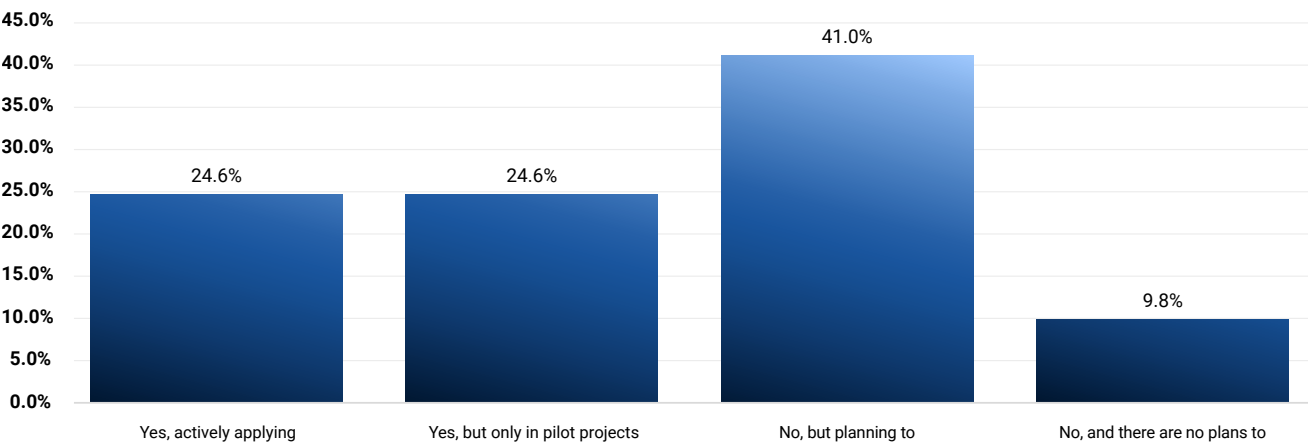
The slower adoption rate is particularly apparent in emerging markets like Vietnam and the Philippines, which appear to be prioritising AI for customer service improvements and other front office functions, leaving areas like compliance and financial crime prevention to take a back seat. “In Vietnam, out of the nine banks I spoke with, only one had its own dedicated AI development team,” Robertson said. “Their focus was entirely on improving customer experience rather than compliance.”

Brent Estrella, Group Chief Compliance Officer at Rizal Commercial Banking Corporation in the Philippines, told Regulation Asia that his bank has more than 50 models that extensively use machine learning, but they are largely focused on customer insights, generating sales leads and other front office activities. The bank is however currently exploring the use of AI to trigger the CDD refresh process, based on specific events and other risk factors. The proposed model is to be trained on historical suspicious transaction reports. [Full interview on [page 19](#)]

“We are seeing an increase in interest for AI-related products as the technology develops further and improves in sophistication.”

Craig Robertson,
Financial Crime SME -
APAC, Financial Services,
SymphonyAI

Application of AI Technologies in AML-Related Activities



I Q&A with Siddhant Sahai



Siddhant Sahai
Stream Lead - Financial Crime
Oversight, Obligations and Controls
Suncorp Bank, Australia

Siddhant Sahai discusses his observations on how FIs are adopting AI in financial crime risk management and some of the core challenges these initiatives face

What have you observed in the industry regarding the use of AI and machine learning to address financial crime risk?

Sahai: There is a maturity curve in terms of the application and uses of AI and technology for financial crime related initiatives. At the high end, I have observed the use of AI-driven network graph analytics to identify hidden relationships, connected parties, criminal gangs, and syndicates and that revolutionises financial crime prevention and suspicious activity detection.

Some large and international banks are using advanced analytics and machine learning for transaction monitoring to improve detection of suspicious transactions and fraud patterns, reduce false positives, and enhance operational efficiency. Given the rising impact of scams and frauds on customers, some international banks are using AI for 'real time' monitoring and detection of fraud risks to prevent incidents.

From the perspective of a domestic bank offering vanilla products and services (e.g. retail lending and deposits), similar technologies can be used but

often by using established third-party technology providers instead of in-house systems – for KYC, screening and transaction monitoring. Banks also apply advanced analytics for assigning customer risk ratings, i.e. to score customers based on certain factors as they emerge, e.g. transaction patterns, geographic risk, customer incidents, etc.

I see an intention and hence an increasing use of machine learning in the industry to ingest large sets of data like customer transaction records to detect suspicious transactions, anomalies in transaction patterns and money mule activity which has impacted the financial services industry in recent years. Similarly, there are efforts to use natural language processing (NLP) to extract text from news articles, social media, web scraping, regulatory filings, corporate registers, and beneficial ownership registers – and then feed these inputs into machine learning models.

GenAI has the ability to detect and inspect vast data sets to detect behavioural anomalies, flag suspicious transactions in real time, and apply 'adaptive learning', though not a lot of FIs have got to the point of full deployment.

“

I see an intention and hence an increasing use of machine learning in the industry to ingest large sets of data like customer transaction records to detect suspicious transactions, anomalies in transaction patterns and money mule activity

Siddhant Sahai, Suncorp Bank

What are the most fundamental challenges involved in deploying AI-based solutions?

Sahai: The biggest underlying challenge lies in data quality, reliability and integrity, and bias in data. Good quality data is necessary for the effective use of AI and machine learning based models. Since traditional (and disparate) systems continue to be used for collecting, managing and storing customer data, FIs need mechanisms in place to ensure that the data they collect is reliable, timely, accurate and that it can be integrated across different systems.

This includes ensuring data lineage, diverse and representative datasets, proper data cleansing, and extraction (without data leakages) to a data lake where it can then be used for performing advanced analytics. You also need your systems to be interoperable to ensure the smooth flow of data in the right format and while maintaining integrity. This is a significant area of work that FIs need to address in order to use analytics meaningfully to identify and detect potentially suspicious transactions that warrant further investigation, develop valuable metrics and Key Risk Indicators (KRIs) for Management Information (MI) reporting, and plan assurance and testing activities.

I also see a need to uplift skills and reduce the talent gap in the industry. More people are needed who have practical experience with data, database structures, analytics and AI systems. Unfortunately, these skills and expertise are often still in short supply in the industry.

Another challenge is around ensuring data protection and privacy, where there is a need to share data both internally and externally, especially when offshored or outsourced. We have to ensure sensitive data is filtered appropriately, especially personally identifiable information. Data also has to be encrypted in this process and only shared on a need-to-know basis.

There is an ongoing and evolving risk of cyber threats and hence ensuring cybersecurity is necessary, i.e. robust access controls, protecting critical infrastructure, and appropriately managing and responding to threats. It's important to ensure our data is secure and that our systems are resilient against cyber threats.

What is the role of regulators in advancing AI innovations in the industry?

Sahai: Currently, since there are no standardised frameworks to address ethics in AI, we need to be cautious about using both real and synthetic data for training AI models to ensure this doesn't result in model bias or discrimination. I think regulators will collaborate at the international level to develop such a framework and there will be more public-private alliances in this regard.

Regarding regulatory guidance, some regulators like the Hong Kong Monetary Authority (HKMA) and the Monetary Authority of Singapore (MAS) have introduced AI-specific guidance to help FIs understand what they should consider from a regulatory perspective when developing use cases.

These currently are more principle-based, but I think this will evolve over time and clarify future approaches to address issues relating to data quality and reliability, ethics, model bias, fairness, explainability, transparency and consumer protection.

I think in some jurisdictions, more could be done by regulators to give FIs flexibility to test and experiment with new technologies, such as by offering innovation sandboxes and facilitating knowledge sharing within the industry where FIs could share successful use cases.

In the long run, FIs should be allowed to pool data (that meets privacy and protection standards) for use in training AI models. This federated learning approach will genuinely help in preventing and detecting financial crime across the industry.

How do you demonstrate the value of investing in AI to secure board and management support and the necessary resources to develop these initiatives?

Sahai: To a degree, there is a certain level of peer pressure that can spring bank boards and senior management into action to invest in and develop AI initiatives. Leaders and senior management need to be able to demonstrate that by applying technology, they can better manage risk and regulatory obligations effectively.

Some of the other factors the board and senior management would consider are the potential long-run cost and efficiency savings, such as through a reduction in the number of tasks that have to be undertaken manually through Intelligent Process Automation. There is also value in terms of competitive advantage when one is demonstrating that you are keeping up with your peers and the industry in the application and use of AI.

Where AI is entrenched, some firms may track metrics such as increases or decreases in customer complaints, a reduction in false positives, manual investigation hours saved, or the number of fraud and scam incidents that occurred and were prevented through certain AI initiatives.

Where do you see the industry's use of AI technologies is heading in the next coming years?

Sahai: I think we will see move to use of conversational AI, which utilise NLP chatbots to intelligently analyse unstructured data, which can serve as educational aids for KYC and transaction monitoring analysts and investigations teams.

Additionally, AI will play a bigger role in streamlining processes by using Intelligent Process Automation (e.g. document ingesting, decisioning, regulatory reporting), and enabling compliance team members to concentrate on higher-level tasks.

I also think federated learning will eventually become more accepted, where FIs come together to, subject to certain data protection measures being in place, jointly train AI models using their combined data sets. The whole industry will benefit and learn from this, and it will help to prevent financial crime more effectively.

Over time, I think the use of AI in predictive analytics will also increase, as this will enable FIs to identify potential risks ahead of time and take preventive measures. In the area of frauds and scams, there is a strong desire within the industry and among regulators to focus on 'real time' detection and prevention rather than recovery of losses after an incident has already occurred.

Disclaimer:

The views expressed are personal and do not reflect the views of Suncorp Bank or any other organisation.

AI Deployment Strategies

The majority of respondents (78%) that said their firms are piloting or implementing AI technologies in financial crime functions are prioritising deployment in transaction monitoring. “Transaction monitoring is a natural fit for AI due to its ability to process vast amounts of data and detect suspicious patterns more efficiently than traditional methods,” Robertson commented, responding to the findings.

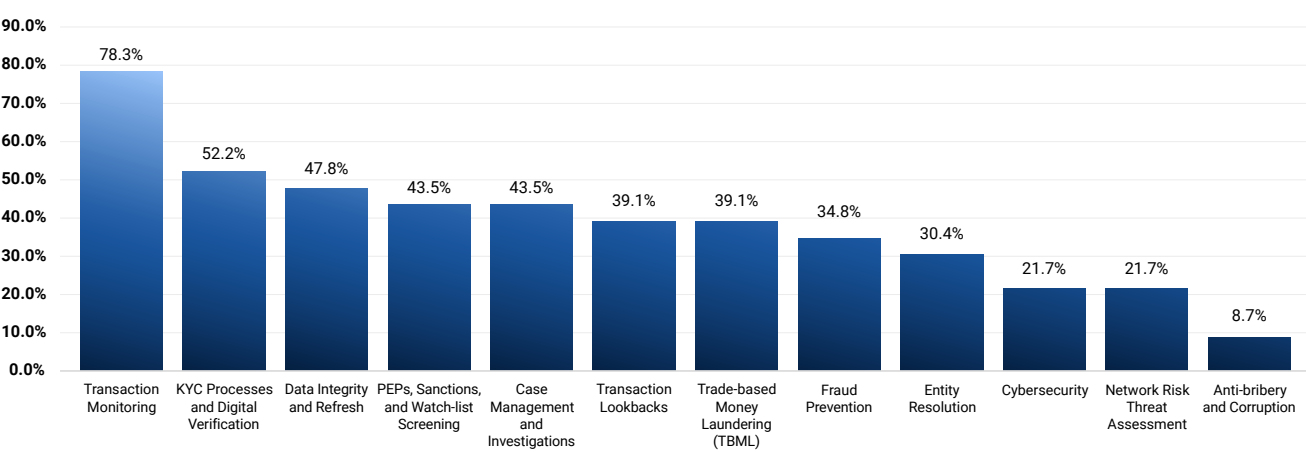
The other top priority areas for AI deployment cited by respondents were KYC processes and digital verification (52%); data integrity and refresh (48%); PEPs, sanctions and watchlist screening (44%); case management and investigations (44%); transaction lookbacks (39%); and trade-based money laundering (TBML, 39%).

According to Maclean, PEPs and sanctions screening is seen as “low-hanging fruit” for deployment of AI technologies, while case management and investigations have always been considered one of the main “high cost areas of financial crime compliance” due to the manual efforts needed for processes like document reviews. “AI can significantly lessen this burden and allow specialists to prioritise better and focus their time on more consequential cases,” he said. “It is not surprising to see TBML as a priority area, given the heavy burden of paper documents imposed on trade finance practitioners.”

As for performing KYC and enhancing data quality integrity, the benefits of AI in improving these processes have been widely recognised, including by regulators such as the Hong Kong Monetary Authority (HKMA). In April 2024, the regulator published [a report](#) specifically pointed to the ability of AI to conduct data quality checks, identify inconsistencies and errors in data, and apply automated cleansing techniques to correct these issues, remove duplicates and standardise data formats.

While the report was focused on improving the performance of transaction monitoring systems in the Hong Kong banking industry, it made clear that data quality enhancements was an AI use case the HKMA supported. More recently in September 2024, the HKMA issued [a circular](#) asking banks to assess the feasibility of adopting AI in their AML monitoring systems and then formulate and submit an implementation plan by the end of March 2025. These were the first instructions to banks by any regulator asking them to study and plan for AI implementation.

Priorities for AI Deployment in Financial Crime Functions



When it comes to AI deployment, the largest number of respondents (39%) reported that their FIs take a “consultative approach”, involving multiple stakeholders from compliance, technology, and business units. Only 6% rely on a “compliance-led” approach, indicating that AI is largely seen as a business-driven initiative rather than a regulatory expectation at this stage.

About 24% of respondents said such decisions were made using a “centralised decision-making” approach, involving a central decision-making body such as a dedicated AI governance board or executive team. Just 6% reported using “decentralised decision-making”, where individual departments or teams can make AI deployment decisions independently and within agreed guidelines. About 24% of respondents said they use a “hybrid approach” with both centralised and decentralised aspects.

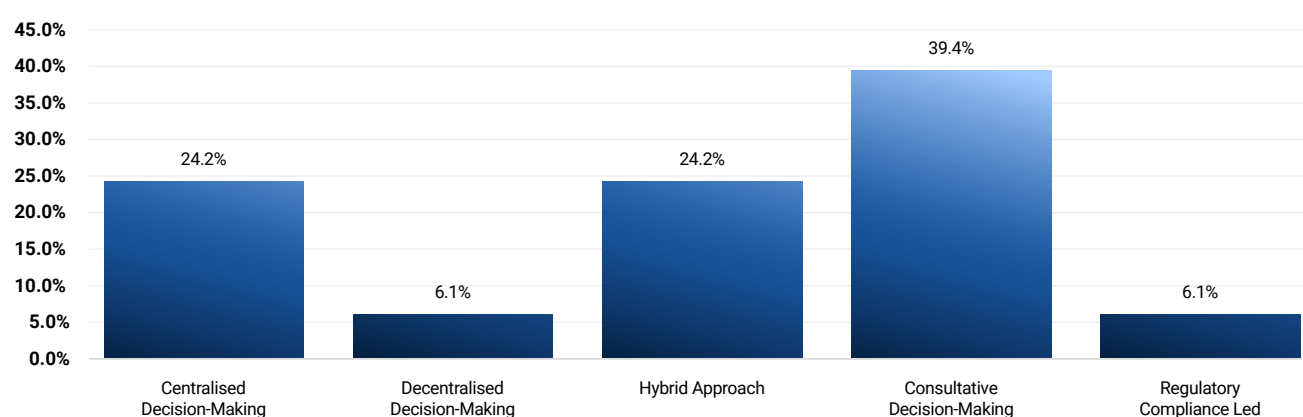
The research highlighted the critical role of the board and senior management in driving AI adoption, with 40% of respondents saying their top leadership are the “primary advocates” for AI adoption, actively setting strategies and priorities. A further 35% of respondents said the board and senior management play an “active supporting” role through resources and policymaking, while 18% said they play a “consultative” role, providing advice and guidance on key decisions. Around 10% of the respondents said the top leadership has “limited” or “no involvement” in AI adoption decisions.

“To a degree, there is a certain level of peer pressure that can spring bank boards and senior management into action to invest in and develop AI initiatives,” said Siddhant Sahai, Stream Lead for Financial Crime Oversight, Obligations and Controls at Suncorp Bank in Australia. “Leaders and senior management need to be able to demonstrate that by applying technology, they can better manage risk and regulatory obligations effectively.”

“Some of the other factors the board and senior management would consider are the potential long-run cost and efficiency savings, such as through a reduction in the number of tasks that have to be undertaken manually through Intelligent Process Automation,” he added. “There is also value in terms of competitive advantage when one is demonstrating that you are keeping up with your peers and the industry in the application and use of AI.” [Full interview on [page 11](#)]

Another research participant said it is much more difficult to advance AI-related initiatives when board involvement is limited or non-existent, and that this can lead to “disillusionment” in many cases. “FIs that fail to align AI strategies with broader business goals risk stalling their AI projects and feeding into the cycle of unmet expectations,” he said, speaking from a Singapore bank.

Decision-Making Approach for AI Deployment and Governance Structure



I Spotlight on GenAI: Opportunities & Risks



15%
of respondents
said they were
actively applying
GenAI in AML
processes, while
a further

26%
said they were
doing so in pilot
projects.

In the financial crime space, GenAI's ability to contextually process, summarise, and analyse vast amounts of unstructured data positions it as a valuable tool for addressing long-standing industry challenges. Despite this optimism, adoption remains in its early stages.

Through this research project, early adopters of GenAI in AML processes reported mixed results. Improvements in areas like suspicious activity reporting (SARs) and data analysis were cited, but some respondents pointed to persistent challenges in scaling these technologies for real-time compliance operations.

One regional bank reported faster SAR generation using GenAI, but that manual verification of critical information sometimes found errors including "hallucinated" text, causing delays in urgent cases, and lowering confidence in the technology. Yet, another respondent working for a large payments firm described GenAI as being "particularly helpful" when large volumes of SARs need to be filed, as the technology can first identify all the SARs with similar characteristics, and then write standardised narratives for all of those "similar" cases before sample checks are conducted and the SARs are submitted.

“

The decision to delay adopting GenAI can stem from a mix of technological, financial, regulatory, and organisational challenges.

The same respondent also discussed the use of GenAI to “cut through the noise” to identify negative news or adverse media articles that are “highly relevant” to case managers and investigators, and synthesise this into information that can be more quickly and easily digested. He said this is being trialled at several FIs, along with a number of use cases involving the use of GenAI for document reviews as part of the CDD process.

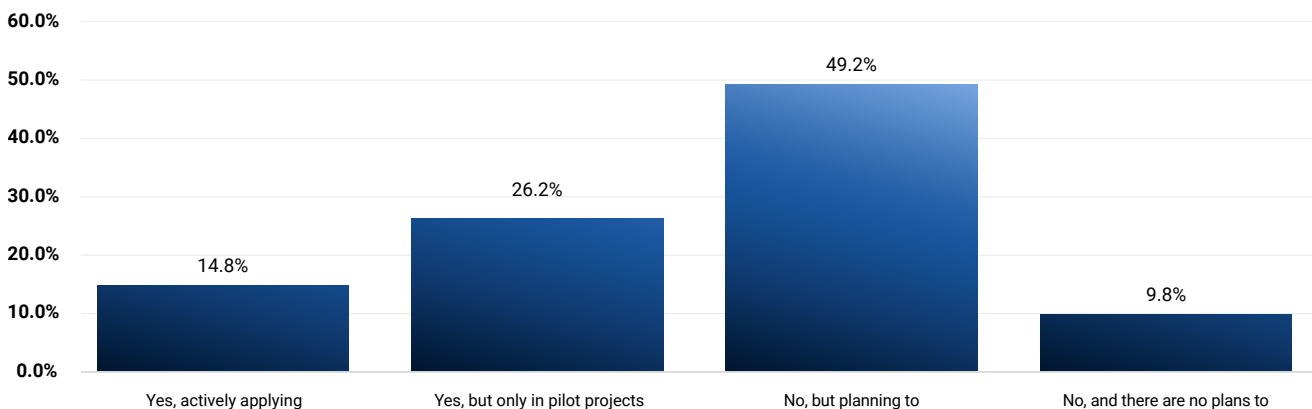
In the research, close to 15% of respondents said they were actively applying GenAI in AML processes, while a further 26% said they were doing so in pilot projects. Almost half (49%) said they were planning to use the technology in future, while just 10% said they had no plans to do so. Globally, this trend is similar. According to the World Economic Forum, 60% of FIs are piloting or deploying GenAI, yet only

around 16% report widespread AI use in compliance operations.

The decision to delay adopting GenAI can stem from a mix of technological, financial, regulatory, and organisational challenges. For the respondents already using GenAI, the most frequently cited use case was for transaction monitoring, followed by alert processing; KYC/CDD processes; and customer risk scoring.

For some firms, the decision is based on the perceived benefits compared to other projects. For instance, RCBC’s Brent Estrella in the Philippines said his bank has “thought about” using GenAI for sanctions screening and writing STR narratives, but that this is “not yet an immediate priority”. This is largely due to manageable alert volumes and a focus on optimising other priority areas first. [Full interview on [page 19](#)]

Utilisation of GenAI Technology in AML Processes



AI Adoption Challenges

Understanding the challenges many FIs face when applying AI in AML provides insight into why adoption is not as high as expected. In the research, the biggest challenges reported by FIs were “Integrating AI with Legacy AML Systems” and “Data Quality and Availability” – both cited in a multi-select question as the top issues by nearly 60% of respondents.

SymphonyAI’s Robertson said he has observed many firms struggling to justify investing in AI when they are still reliant on legacy infrastructure. “There’s a real risk of over-promising and under-delivering when it comes to AI,” he said. “Many firms still see AI as a long-term project, especially when they hit the complexity of integrating AI into legacy systems. Data integrity also continues to be a major focus in our conversations. Organisations should absolutely think long-term but they should also be aware how easily effective AI can be when implemented to deliver a low-impact outcome and without much process upheaval in the short term.”

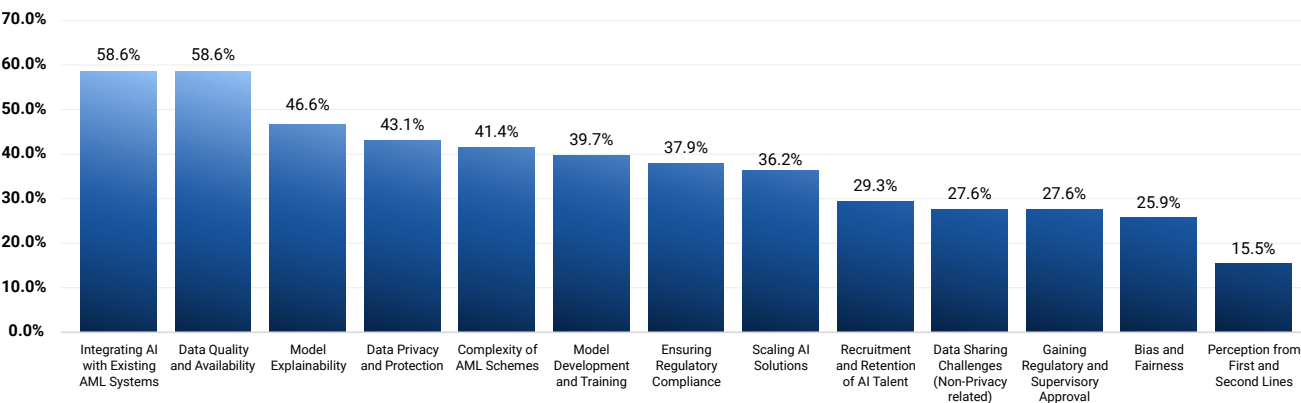
The data-related challenges cannot be understated, as AI is unable to effectively function without good-quality data. Suncorp’s Sahai said data quality, reliability and integrity is the “biggest underlying challenge” when it comes to AI adoption, and that this is a “significant area of work” that every FI needs to address to effectively and meaningfully use the technology.

Another respondent spoke about having to “start from scratch” to create a data governance framework, because his bank did not have one. One respondent described a two-year-long process that it took for his firm to reach a point where its data could be used in an AI project.

Some respondents recognised that AI itself can help address these challenges by automating data cleansing and structuring processes, reducing the time and effort needed. AI tools can detect inconsistencies and anomalies, speeding up the data preparation process and allowing FIs to deploy AI more quickly. This dual role of AI – both as a user and enabler of high-quality data – demonstrates the technology’s potential to overcome key barriers to adoption.

Model explainability, data privacy and protection, model development and training, and regulatory issues were also among the top challenges cited by respondents. Around 43% said data privacy and protection rules were among their top challenges, while 38% cited difficulties ensuring compliance with existing regulatory requirements for FIs; and 28% said they struggled to gain regulatory or supervisory approval for their AI initiatives.

Top Challenges of Implementing AI for AML



I Q&A with Brent Estrella



Brent Estrella
Group Chief Compliance Officer
Rizal Commercial Banking Corporation
Philippines

Brent Estrella discusses RCBC's approach to the use of AI and machine learning and how decisions are made to develop these initiatives.

Are you currently adopting AI in the financial crime space or other areas?

Estrella: We have more than 50 models that extensively use machine learning. These are largely focused on customer insights, generating sales leads and things like that.

So far there have been fewer AI initiatives in the fraud and financial crime space. But one of our first steps in this space is to develop a model that will allow us to operationalise a trigger event-based, dynamic CDD refresh process.

This is partly driven by regulatory requirements to perform ongoing CDD. But it's also driven by resources in terms of how big the teams are that can actually undertake CDD reviews.

I am not a believer of the current approach most banks take of performing periodic CDD reviews at set intervals, as these tend to only come up with the same conclusions that you've had at the last time that you did the review.

In fact, about two years ago we estimated that we would need to hire more than 500 CDD analysts if we were to take the traditional approach of conducting periodic reviews at fixed intervals.

We wanted to move away from just throwing bodies at this task and come up with something which is trigger based.

Two years down the line, we're now at the point where our compliance and data science teams are exploring how we can build a model that will help us deliver that.

How do you envision that using AI in your ongoing CDD process will help the bank?

Estrella: Part of the discussion we've had is that the customer risk rating model we've had in place for the past six years is not quite as advanced as we would like it to be.

We decided we wanted to use AI in order to scale up our customer risk assessments. For example, CDD refresh triggers could be the client's product utilisation history and risk factors that become evident during the relationships.

We decided to look at ways to use partially redacted suspicious transaction reports to train an AI model to look into the demographics and attributes of

customer accounts that we have investigated and found to be suspicious.

We believe this will give us a better way of risk-rating customers from an AML perspective.

What initial foundational challenges did you have to address to get to a point where you were able to manage AI models?

Estrella: We had to start with the most fundamental issues, like establishing a data governance framework. We have since written out a document clearing stipulating our data governance framework, covering all the different kinds of data and the roles of data owners, for example.

This serves as the foundation for us to harness the power of data down the line. Previously, a significant amount of the data was unstructured, much of it on paper and not discoverable. Getting this into a system to make it usable in our models was quite a challenge.

The process of establishing a data governance framework was not easy. Just agreeing on the responsibilities across the organisation was in itself like a Herculean task. But ultimately it was necessary to go through that painful journey to make sure that it was done right.

“

We wanted to move away from just throwing bodies at this task and come up with something which is trigger based.

Brent Estrella, RCBC

How are decisions made regarding the deployment of AI initiatives?

Estrella: We are fortunate to have a CEO who is a firm believer in the power of data and AI. And he has people like myself and my other peer group heads who likewise believe the same. So there is absolute alignment between the department heads and management.

Not to be forgotten is the board. We have a very supportive board in terms of us going down this route. One of our independent directors happens to be the head of the Centre for AI Research in the Philippines, which allows for very good alignment within management.

Of course, there tends to be a natural bias for business related uses of AI or machine learning rather than compliance. So this means that using such technologies in compliance functions can take longer.

But I've found that it is important for people at my level to assert ourselves and communicate our interest in data and technology.

One thing that will help us drive our agenda is having more specialised technical skill sets within the compliance function. This would allow us to pursue this journey from within, rather than having to compete for resources from our bank's data science team.

How do you articulate to the board the value of investing in AI initiatives for risk and compliance functions?

Estrella: As a starting point, our board believes in the principle that compliance is a competitive advantage and is very much engaged on risk and compliance matters. With that alone, you can really go quite far in terms of what investments the bank will actually make into compliance.

In terms of metrics, it's quite difficult to measure the benefits of AI in terms of additional revenues or higher profits, especially in compliance.

But ultimately, our goal is to obtain a perfect supervisory rating, which means that our board is always prepared to make the necessary investments to get us there.

Have you started exploring the use of GenAI within your organisation?

Estrella: We have thought about using GenAI for sanctions screening and for writing STR narratives, as this would free up staff and speed up case management system and decisioning.

But we feel this is not yet an immediate priority right now, because our alert volumes are still at a level that our staff can manage well.

If you talk to a global bank with significantly greater volumes of alerts and regulatory pressures from different corners of their operations, then it's probably going to be a very different conversation.

What drives decisions and appetite to spend on GenAI adoption?

Estrella: It's really a revenue conversation. For now, GenAI is really more of an optimisation, and there are many other areas for optimisation that are seen as higher priorities.

But to be fair, if there was a use case for GenAI that we really felt we needed, for example to satisfy a regulatory concern, then our bank would not hesitate to make that move.

“

The process of establishing a data governance framework was not easy. Just agreeing on the responsibilities across the organisation was in itself like a Herculean task. But ultimately it was necessary to go through that painful journey to make sure that it was done right.

Brent Estrella, RCBC

What steps is Bangko Sentral ng Pilipinas (BSP) taking to ensure AI is adopted responsibly in the banking industry?

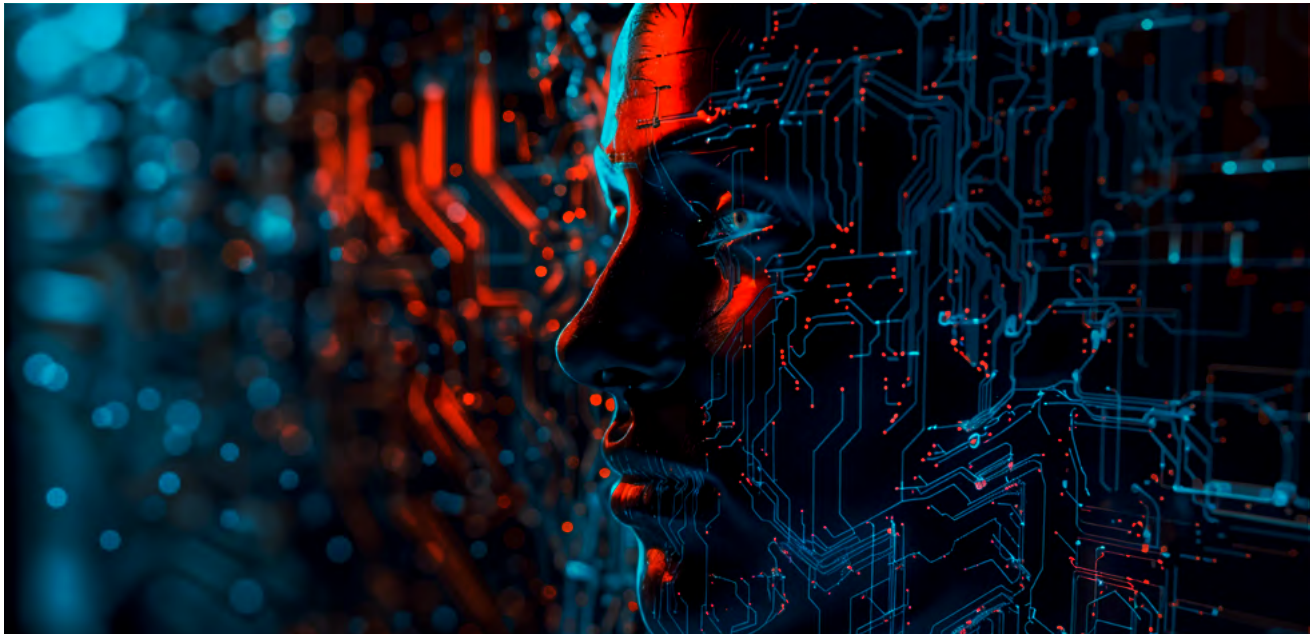
Estrella: The BSP conducted a thematic review to understand how some of the banks are using AI. Our bank was included as one of the participants in this review.

Based on the findings from this review, the regulator is developing a framework for the industry focusing on the use of AI. This is currently expected to be released before the end of this year.

Beyond that, whenever we get a sense that there could be a regulatory issue, we are able to adopt a sandbox approach with our regulators.

This means going to talk to the regulator and explaining what we are planning, and asking them to allow us to experiment within a sandbox.

AI Value Articulation



The most common metric to communicate value of AI applications in AML operations was the false positive rate, cited by 61% of respondents.

Understanding the cost and benefit to the business is an important step for FIs in any AI journey, particularly in an economic climate that has firms becoming increasingly cost-conscious. In many cases, where FIs are deploying AI, it is in revenue-generating areas such as sales and marketing rather than compliance. Therefore, a strong business case has to be communicated to secure board and senior management buy-in and the resources necessary to pursue AI initiatives for AML-related functions.

In the research, respondents were asked about the metrics they use to measure the effectiveness of AI applications in AML operations and how they communicate value of these initiatives to their top leadership. The most commonly

(61%) cited metric was the false positive rate. High false positives generated by transaction monitoring and screening systems have long been a burden on FIs, particularly those with large global footprints and significant cross-border business.

For most FIs, false positives take significant time and manual effort from case managers and investigators to clear. Further, false positives can create negative experiences for customers, slow business growth, and hinder efforts to address genuine money laundering concerns. FIs that can make the case for lowering false positive rates using AI are therefore more likely to be successful in securing board and management buy-in.

“

In markets like Hong Kong, compliance costs are sky-high, and AI is seen as a way to reduce those costs.

Craig Robertson,
Financial Crime
SME - APAC,
Financial Services,
SymphonyAI

Accuracy rate (52%) was the second most commonly cited metric used to demonstrate the effectiveness of AI projects, followed by efficiency improvements (46%), detection rate (44%), and cost savings (43%). These metrics, when shown to be improving, all mean that compliance officers, case managers and investigators are freed up to focus on higher-value activities and cases.

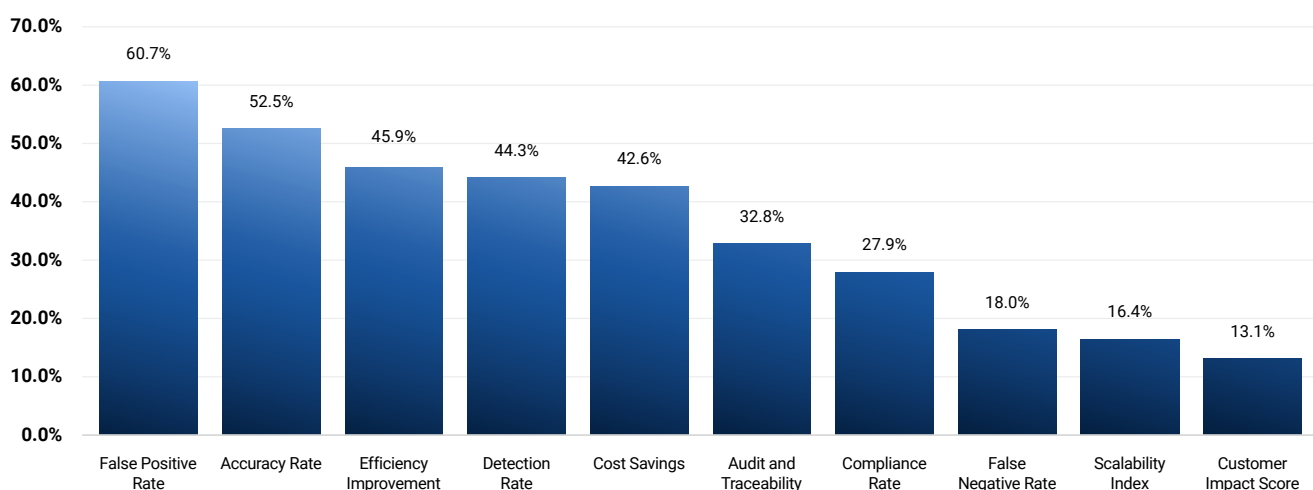
While AML compliance functions have to demonstrate cost-savings, front office functions demonstrate the revenue opportunity, arguing a more powerful driver of board and senior management support. According to Regulation Asia's Brad Maclean, those working in AML roles should emphasise the importance of financial crime

compliance when communicating the value of their AI projects, which can include discussions on the legal, regulatory and reputational risks associated with non-compliance and detection failures.

Many respondents in developed markets like Australia, Singapore, and Hong Kong, where the cost of compliance is considered significant compared to less developed markets, report that they seldom experience pushback from boards and senior management for AI projects aimed at enhancing their financial crime risk management capabilities. In part, this is due to support from regulators in terms of regulatory guidance and the high priority placed on guarding against money laundering and other types of illicit finance activities.

“In markets like Hong Kong, compliance costs are sky-high, and AI is seen as a way to reduce those costs,” said Robertson. “In some other markets, we’ve seen firms struggle to align their AI objectives due to a lack of regulatory guidance. The technology moves faster than the regulations, so firms can be hesitant to invest heavily without clearer guidance from regulators. But it is imperative that firms prioritise and communicate the importance of enhancing the efficiency and effectiveness of their financial crime controls and systems.”

Metrics Used to Measure Effectiveness of AI Applications in AML



I Q&A with Dr. Elea Wurth



Dr. Elea Wurth
Lead Partner Trustworthy AI
Strategy, Risk & Transactions
Deloitte, Australia

Dr. Elea Wurth discusses the maturity of AI in Australia's financial industry and how firms should go about developing their governance frameworks.

How mature is Australia's financial services sector when it comes to implementation of AI?

Wurth: Australia is generally lagging globally when it comes to AI innovation and deployment for value. Financial services demonstrate the full range of ambition, where some see AI as integral to their future and others retain a 'bricks and mortar' strategy.

Certainly some of our larger banks are highly progressed in this space, but as an industry, I would say that financial services is not a front runner in either maturity of implementation or AI governance.

What are the main use cases FIs are prioritising when it comes to financial services?

Wurth: In September, the government proposed mandatory guardrails for AI in high-risk settings, which essentially gave us an indication of what AI regulation is going to look like for high risk AI.

There's certainly some FIs looking to implement AI for AML, but AML and many of the customer facing AI solutions would be considered high risk

under the Australian definition, so there is a higher requirement for risk management and governance around these kinds of use cases.

We've found there's a bit of reticence in the financial industry to move towards customer facing or high risk AI models without really understanding what the regulation will be, and how to effectively manage the risk of those models.

So what we tend to see is that early AI deployment within financial services is internal facing, like back office operations. These deployments tend to focus on productivity and efficiency gains internally in back office rather in customer facing functions at this point.

What are the key areas FIs should focus on when it comes to AI governance?

Wurth: When we talk about governance, we're talking about frameworks set up to protect the organisation, their customers, society, and ensure they are adhering to the appropriate emerging regulations, corporate policies, and societal expectations, for example.

Firms should make sure they're implementing a governance system that gives visibility and control of AI procurement, deployment, and use within the organisation, covering the users of the AI system all the way up to the board.

When you're looking at developing those governance structures, the focus should be on ensuring that your AI is ethical, is lawful, and is accurate. Accuracy refers to the AI being technically robust, that it's doing what you think it's doing.

It is incredibly important to be able to define your ambition and AI strategy upfront to help define what your AI governance needs actually are. Some organisations have very simple ambitions, such as to allow their staff to use publicly accessible GenAI tools like ChatGPT. In these cases, you don't need an enormous in depth, complex governance structure

How do firms with larger AI ambitions tend to go about developing their governance frameworks?

Wurth: Organisations with larger ambitions may go ahead and develop AI use cases and build out their POCs and POVs. In some cases, it is only when they actually get to the point of wanting to deploy into production that they suddenly realise they don't have any way to manage the risk.

This can be a blocker to achieving value from AI, because no executive or board is going to provide the approvals or the funding to go into production if they don't feel comfortable that the AI programme is being effectively risk managed and appropriate safeguards are in place.

“

So what we tend to see is that early AI deployment within financial services is internal facing, like back office operations. These deployments tend to focus on productivity and efficiency gains internally in back office rather in customer facing functions at this point.

Dr. Elea Wurth, Deloitte

Other organisations are more risk averse, so they tend to focus on developing their AI risk frameworks and governance before they start investing in innovation, so they can feel comfortable in that investment and innovation. That's another extreme.

The most effective organisations tend to develop their AI strategy and governance frameworks in unison. By the time they get to a point where they've gone through their development and experimentation phase, they've also already built out safeguards and risk management along the way, so they're immediately ready to move into productionisation and value achievement.

How do firms go about measuring and demonstrating that their AI programmes are achieving value?

Wurth: It's incredibly important to have value measurement in place upfront. Many organisations will go forth and develop and invest in AI programmes without really understanding the value that they need to be achieving.

Organisations should not be looking to procure, develop, or deploy AI just for the sake of having AI. There needs to be a real focus on what is the value metric for your AI programme. This needs to be set clearly upfront, and there should be regular check-ins to make sure those value metrics are being achieved.

So when we're looking at AI strategy and governance, value management and setting those metrics upfront is absolutely a key component of any AI programme.

What should governance look like for firms that are using AI developed by third-party firms rather than in-house?

Wurth: Even if you're buying off the shelf and you're going with a major provider, as the deployer of that AI, you are responsible for any risk that is realised from the deployment.

So you still need to have a governance framework, the same as you would if you were developing your AI internally. No matter where you are on that journey, you need to have your own risk assessment in place, and ensure that you manage the risks appropriately.

You would still need to right-size your AI risk management governance, so there would be some differences for those developing AI internally vs deploying from external providers.

“Organisations should not be looking to procure, develop, or deploy AI just for the sake of having AI. There needs to be a real focus on what is the value metric for your AI programme. This needs to be set clearly upfront, and there should be regular check-ins to make sure those value metrics are being achieved.”

Dr. Elea Wurth, Deloitte

I Regional Regulatory Snapshot



The regulatory landscape for AI in Asia is rapidly evolving, with various countries taking significant steps to define how AI should be deployed, particularly in financial services. While the enthusiasm for AI's transformative potential is evident, the lack of unified frameworks across the region presents both challenges and opportunities.

1. Singapore: Leading in AI Governance with a Balanced Approach

Singapore has positioned itself as a frontrunner in AI regulation, led by the Monetary Authority of Singapore (MAS), which emphasises ethical AI adoption through its Fairness, Ethics, Accountability, and Transparency (FEAT) principles. The Veritas Initiative further helps FIs ensure that their AI processes comply with governance and ethical standards. Singapore's AI Governance Framework, driven by IMDA in coordination with industry via the AI Verify Foundation, also promotes transparency and security, setting the benchmark for balancing innovation with regulatory oversight.

2. Hong Kong: Emphasising Transparency and Accountability

Hong Kong's regulatory landscape focuses on ensuring transparency and accountability in AI adoption, particularly through frameworks like the Personal Data (Privacy) Ordinance (PDPO) and the initiatives led by the HKMA. The AI Supervisory Sandbox allows FIs to test AI-driven anti-fraud and AML technologies in a controlled environment. The HKMA has recently become the first regulator to instruct FIs to assess the feasibility of adopting AI in their AML monitoring systems and then submit implementation plans to the regulator.

3. Japan: Cautious but Focused on Accountability

Japan's approach to AI adoption is more conservative. The Financial Services Agency (FSA) emphasises transparency and accountability, ensuring AI does not compromise consumer protection or contribute to discrimination. Although AI use in financial crime compliance is still in its early stages, Japan's ethical guidelines and clear privacy laws ensure a secure regulatory foundation as FIs gradually adopt the technology.

4. Australia: Mandatory Guardrails for AI

Australia is proposing to introduce mandatory AI guardrails and voluntary standards to ensure ethical AI deployments in high-risk sectors, including financial services. The Australian Government's AI Ethics Framework emphasises consumer protection and system integrity, with guidelines focused on transparency and risk management. Released in 2024, Australia's regulations are a significant step toward integrating AI with clear governance structures.

5. Malaysia: Plans for AI Hub with a Focus on Regulation

Malaysia has announced plans to rapidly position itself as a key player in AI development, with its recent initiative to establish itself as a regional AI hub. The strategy focuses on driving AI adoption across industries, particularly financial services. Regulatory frameworks are being shaped to align with global standards and support AI innovation while ensuring risk management around data privacy, transparency, and accountability.

6. Vietnam: Draft Law on Digital Technology and Data

Vietnam is advancing its AI and data governance regulatory framework by introducing laws on digital technology and data, focusing on enhancing data privacy, security, and transparency. A notable feature of these laws is data localisation, requiring certain types of data collected in Vietnam to be stored locally, which may affect cross-border AI applications. In June 2024, Vietnam's Ministry of Science and Technology issued nine principles for research and development of responsible AI systems and guidelines for implementation.

7. China: First Mover with GenAI-Specific Framework

China has positioned itself as one of the first markets to move on GenAI regulation, introducing GenAI-specific frameworks in 2024. These

frameworks align with the country's broader data security, data privacy and cybersecurity laws, focusing on content control and accountability in AI deployment. China's approach includes strict guidelines for AI-generated content and mandates clear human oversight in high-risk sectors, making it one of the first countries to comprehensively regulate GenAI.

8. Indonesia: Balancing Innovation with Strong Regulatory Oversight

Indonesia is actively developing its AI regulatory framework to balance innovation with strong oversight. The Ministry of Communication and Informatics (Kominfo) has introduced guidelines emphasising ethical AI adoption, transparency, and accountability. Indonesia's National AI Strategy focuses on driving AI innovation while ensuring robust governance structures are in place. The country is also exploring the establishment of an AI sandbox to allow FIs to test the technology in a controlled environment, and preparing to issue a ministerial regulation on AI.

9. Thailand: Emphasising Data Privacy and Security

Thailand is enhancing its AI regulatory landscape with a strong focus on data privacy and security, with the Electronic Transactions Development Agency (ETDA) and the National Digital Economy and Society Committee (NDESC) leading the effort. Thailand's Personal Data Protection Act (PDPA) ensures strict data protection measures, while the AI Governance Framework emphasises transparency, fairness, and ethical AI deployment. Thailand's government is also encouraging the development of AI ethics committees within organisations to oversee AI implementation and compliance, with policymakers planning to draw up new AI rules to prevent the ethics violations.

10. Philippines: Building AI Capabilities with a Focus on Emerging Regulation

The Philippines is in the early stages of AI development, with several pilot projects in the financial services sector focusing on fraud detection and compliance. Broader integration across other industries is still in its infancy, with significant investment still needed required to support large-scale AI adoption. The Philippines is actively working on draft legislation focused on areas such as data privacy, cybersecurity, and the ethical use of AI. The central bank is meanwhile working on AI guidelines for the banking sector. The Philippines has also proposed the introduction of a comprehensive AI regulatory framework for the ASEAN region by 2026, covering cybersecurity and GenAI, among other areas.

SymphonyAI's Commitment to Responsible AI

SymphonyAI is a leading enterprise AI SaaS company for digital transformation across the most critical and resilient growth verticals including financial services. The firm is focused on ensuring responsible AI practices in its enterprise AI solutions, placing emphasis on maintaining data integrity, mitigating bias, and promoting fairness in AI systems.

This approach addresses key regulatory considerations and enables real-time feedback, which is critical in regulated industries. By integrating human oversight, SymphonyAI aims to ensure AI decisions are reliable and aligned with operational standards.

SymphonyAI's Five Responsible AI Principles are:

- 1. Accountability:** AI systems should be designed and operated in a way that ensures stakeholders can hold product users responsible for their actions and decisions.
- 2. Transparency:** Their decision-making processes and potential biases must be clear, understandable, and open to customers, developers, and regulators.
- 3. Reliability & Safety:** They should behave predictably and within customer and industry acceptable risk thresholds to ensure customer trust and confidence.
- 4. Security:** Security of information and systems, of both SymphonyAI and its customers, must be maintained and sustained throughout the full AI system and data lifecycles.
- 5. Privacy:** SymphonyAI adopts the principle of Privacy by Design. All AI systems designed, developed, implemented, maintained and decommissioned must meet the requirements of applicable laws, regulations and industry standards.

By adhering to these principles, SymphonyAI ensures that its AI technologies are not only innovative and effective but also secure, and adaptable to evolving regulatory frameworks, standards, and best practices. This commitment fosters trust and confidence among stakeholders, supporting responsible and sustainable AI adoption across industries.

Final Thoughts & Strategic Recommendations

Final Thoughts:



GenAI adoption in financial crime compliance across Asia Pacific FIs has been slow, with most firms still navigating the complexities of traditional AI implementations. Legacy AML systems, data quality issues, and a fragmented regulatory landscape have further hindered progress. While there is growing interest in AI, the majority of FIs remain in the early stages of deployment, focusing primarily on customer-facing applications rather than compliance.

However, the urgency to embrace AI in compliance functions has never been greater. Recent high-profile financial crime cases

have exposed vulnerabilities in traditional compliance systems, highlighting opportunities where AI and GenAI could have played a more significant role in identifying and mitigating risks earlier. For financial crime compliance teams, leveraging these cases to outline the clear gaps and inefficiencies in current systems can drive stronger buy-in for AI programmes.

In Japan, a criminal organisation called the 'Rivaton Group' was caught using 500 shell companies and 4,000 bank accounts to launder JPY 70 billion (USD 470 million) of illicit proceeds in the first half of 2023. The banks that opened those accounts were not able to detect links between the accounts or identify that transfers made to online casinos and overseas corporate accounts were suspicious. The FSA issued directions to FIs in September 2024 outlining a series of measures they are expected to take to improve customer verification, behaviour analysis, transaction monitoring, and detection scenarios, among other areas.

In Singapore, ten foreigners were arrested in August 2023 and charged for money laundering related crimes. About SGD 3 billion (USD 2.3 billion) in assets

“

AI-driven solutions offer not just operational efficiency but significant effectiveness improvements in detecting and preventing complex financial crimes, which represent significant competitive advantages in today's environment.

are involved in the case. While the ten individuals were ultimately convicted and jailed, multiple Singapore banks have been under scrutiny for failing to detect false documents during onboarding. The MAS has directed banks to improve their processes for verifying sources of wealth (SOW), and plans to impose fines and other punitive measures on some of the banks that had dealings with the ten convicts.

These two high-profile financial crime cases identify system and control deficiencies that can already be enhanced with current AI technologies, including customer verification, behaviour analysis, transaction monitoring, and false document detection. With regulators already directing FIs to fix these areas, the case for leveraging AI to gain efficiency in the process makes for a stronger case when trying to secure buy-in from stakeholders.

By demonstrating how AI can address critical gaps – such as enhancing detection accuracy, reducing false positives, and speeding up response times – FIs can turn these challenges into opportunities for technological advancement and a more refined approach to risk management. This improves operational efficiency and deepens the ability to understand, anticipate, and mitigate risks, offering a more proactive stance in the ever-evolving landscape of financial crime.

The ability to leverage AI for a better grasp on risk factors transforms compliance efforts into a strategic asset for FIs, enabling them to predict and curb risks before they manifest into potentially reputation-damaging events. This move from reactive detection to proactive prevention will mean better outcomes for consumers and the FIs themselves, avoiding the cumbersome process of tracking down and trying to recover funds after they have already undergone various sequences of cross-border transactions.

Moreover, with growing goodwill and interest from boards and executive leadership in investing in AI and GenAI programmes, now is the time for compliance teams to present the case for scalable AI solutions that address today's risks and position the FI to proactively combat future threats. AI-driven solutions offer not just operational efficiency but significant effectiveness improvements in detecting and preventing complex financial crimes, which represent significant competitive advantages in today's environment.

The shift from traditional methods to AI-driven solutions is no longer optional – it is essential for the future of financial crime compliance. To capitalise on the full potential of AI, FIs must be proactive, strategic, and forward-thinking.

Strategic Recommendations:



The recommendations set out below aim to address the key takeaways from the research and provide a roadmap for effective AI adoption and integration within FIs.

1. FIs should begin with small-scale AI pilots, without committing significant resources, conducting low-impact tests to understand the technology's capabilities and limitations against concise criteria for measuring success. These deployments can be gradually scaled up, ensuring that each stage builds on the successes and learnings of the previous one, including to address data quality issues and challenges associated with legacy system integration.
2. FIs should engage openly with regulators to demonstrate the progress and effectiveness of their AI initiatives, while also showcasing the benefits and risk management capabilities of these initiatives to build regulatory confidence in the technology. Technology providers should be expected to partner with firms to engage with regulators to explain AI design and ethics principles. Overall, engagement with regulators should be framed to help shape guidance for the wider regulated population and promote proactive and bold steps to drive these outcomes.

3. FIs should from an early stage start with goals of improving operational efficiency, and then define their next set of goals to include reinvesting some efficiency gains into model risk governance and financial crime risk management. In practical terms, FIs should use the time and resources saved to focus on enhancing controls to prevent financial crime and look across case work to better understand the vulnerabilities being exploited by criminal actors and use those findings to improve AI models.

4. FIs should consider using AI technology to enhance data quality and governance practices, including to address common challenges with data lineage and streamline processes associated with data collection, cleansing and transformation. This will reduce the size of investment in data management, while promoting better governance practices, and freeing up time and resources to plan and execute digital transformation initiatives to improve financial crime prevention capabilities.

5. FIs should implement robust governance and accountability frameworks to support AI adoption and develop clear metrics to measure the success of AI initiatives. This includes ensuring boards and senior management engage in and understand the value and benefits of AI in compliance functions and how risks are managed, which will help to secure strong sponsorship from leadership. An additional outcome of the top-line sponsorship is enhanced engagement with regulators to promote guidance and support for AI adoption in financial crime risk management.

With these factors in mind, FIs need to prioritise proactively scaling their AI and GenAI capabilities to stay ahead of the curve. FIs that can position AI as a critical solution and secure board-level commitments to sustained investment in AI technologies will not only build long-term resilience and build competitive advantage, but also demonstrate their leadership in helping to define the future of financial crime compliance.



I About SymphonyAI

SymphonyAI is a leading enterprise AI SaaS company for digital transformation across the most critical and resilient growth verticals, including retail, consumer packaged goods, financial services, manufacturing, media, and IT/enterprise service management. SymphonyAI verticals have many leading enterprises as clients. Since its founding in 2017, SymphonyAI has grown rapidly to 3,000 talented leaders, data scientists, and other professionals. A 2024 Microsoft Partner of the Year for Business Transformation – AI Innovation, SymphonyAI is a SAIGroup company, backed by a \$1 billion commitment from successful entrepreneur and philanthropist Dr. Romesh Wadhvani.

Learn more at:

 www.symphonyai.com

 <https://www.linkedin.com/company/symphonyai/>

Contact us at:

Craig Robertson

Financial Crime SME – APAC

Financial Services

SymphonyAI

Kim Yu

Head of Marketing – APAC

Financial Services

SymphonyAI

kim.yu@symphonyai.com

I 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.

Learn more at:

 www.regulationasia.com

 <https://www.linkedin.com/company/regulation-asia-regwire/>

Contact us at:

Bradley Maclean

Co-founder & Editorial Director

Regulation Asia

brad.maclean@regulationasia.com

