Intelligent compliance

Financial crime compliance experts call for a smarter approach, built on technology innovation, information-sharing, risk-based policies and common sense.

> **The challenge that bedevils the industry is the gap between technical and effective compliance.**
>
> **Alan Ketley,** Bank of Tokyo Mitsubishi UFJ

The challenges of moving beyond purely 'legalistic' compliance with financial crime regulations were high on the agenda in the opening session of Sibos 2017's compliance stream, 'Counter-terrorist financing – Are we really stopping the bad guys?'

The quantum leap in compliance requirements since 9/11 has led to banks spending much of the past 15 years implementing processes to adhere to laws passed to starve terrorists of funds. In many respects, these efforts to close off the financial system to terror financing have been successful. As panellists noted, ISIS cannot use the financing techniques that supported Al Qaeda.

> **Banks are using sophisticated analytics to tune their models for matching purposes.**
>
> **Vikas Agarwal,** PwC

The increased incidence of lone wolf attacks, funded by small sums, channelled via legitimate means such as student loans, reflect the increased difficulties facing terrorist organisations, but also represent a new challenge to banks, regulators and law enforcement agencies.

"From a public policy perspective, the greatest utility is in understanding the use of the financial system in the formative steps of a lone-wolf attack. There is more value in building up intelligence on suspects, than refusing to permit a $30 van rental," said Mark Gem, head of compliance at Clearstream and chair of the International Securities Services Association's financial crime principles working group.

Measurable objectives

But the emergence of new threats – including cyber-security attacks by state actors – underlines the reality that success is temporary but the need to improve defences permanent. Moreover, whilst responding to new modus operandi, banks are under pressure to improve both the cost-efficiency and effectiveness of their compliance efforts.

"The challenge that bedevils the industry is the gap between technical and effective compliance. Banks can execute perfectly on well-written policies and procedures. But if they're looking in the wrong place, they're not being very effective," observed Alan Ketley, managing director for anti-money laundering (AML) strategy at Bank of Tokyo Mitsubishi UFJ.

In a field where success is hard to define other than as the absence of failure, should we change our KPIs, asked moderator Kavita Maharaj. "How do you assess in real-time activities that are likely to look strange with the benefit of hindsight? In sales, I had a sales quota. In compliance, we report. US and European banks file two million suspicious activity reports every year, but Europol estimates that 10-12% of those from European banks are progressed," said Ketley.

This core challenge threaded through a varied two-day programme. For an industry in which measurable results are essential, the difficulties of calculating a return on investment in compliance staff and technologies are frustrating. This problem is all the more acute when those investments run collectively into billions, with little prospect of a reduction.

But while cost is a factor, effectiveness of compliance efforts was always front of mind for panellists. Thus, measurable objectives, improved skillsets, new technologies, risk-based strategies and increased information-sharing were common themes across all sessions.

Divergent signals

Speakers recognised that a shift to a more targeted, risk-based approach to financial crime compliance demanded greater information-sharing between banks, regulators and law enforcement agencies.

In 'The future of financial intelligence sharing', panellists discussed the potential offered by an emerging form of public-private sector collaboration: financial information-sharing partnerships (FISPs). First developed in the UK, six FISPs are now in operation (Australia, Canada, Hong Kong, Singapore, US and UK), with most G20 countries planning to follow suit, according to Nick Maxwell, head of the Future of Intelligence Sharing Programme at the Royal United Services Institute.

Essentially voluntary forums, FISPs facilitate increased dialogue and information-sharing between major banks, regulators and law enforcement agencies, to deepen collective understanding of current and emerging threats, albeit with

their precise terms defined by national legal frameworks. While asserting the scope for FISPs to help banks better tailor their efforts, Maxwell identified five priorities for their sustained development: leadership and trust; legislative clarity; governance; technological and analytical capability; and adaption and evolution.

Maxwell placed particular emphasis on the importance of political will, both in terms of resources and legislation. "With the introduction of the new European General Data Protection Regulation – which has extra-territorial implications – regulated entities are being given divergent signals by policy makers," he said. "We should not incentivise data protection without a conscious understanding of how it will affect the financial crime regime."

While other panellists raised similar concerns over the difficulties raised by data protection regimes, Clearstream's Gem noted that Europe's Fourth Anti-Money Laundering Directive represented a shift from a rules-based to a risk-based approach.

Risk-based approach

In parallel with efforts to improve effectiveness, banks are looking for enhancements across process, people and technology to improve best practice. In 'Future trends in sanctions – can automation, artificial intelligence (AI) and outsourcing resolve inefficiencies?', Lorraine Lawlor, director of sanctions governance at Wells Fargo, called for process overhaul to reflect the complexity and effort involved in screening against regularly updated sanctions lists from multiple governmental entities.

"We still need to be screening our transactions and customers, but I do think we need to rethink how we're doing this," she insisted. "I think sanctions compliance is turning more into an AML model. The two disciplines are merging. It's a due diligence issue: Do you know your customers, and what are the risks associated with them dealing with someone you don't want them to be dealing with? We need to have a truly risk-based approach rather than today's catch-all approach."

New technologies have potential to reduce current inefficiencies, according to Vikas Agarwal, principal in the financial services risk, regulatory and financial crime technology practice at PwC, citing three prime examples.

"First, banks are using sophisticated analytics to tune their models for matching purposes; second, they are using machine learning to improve data quality, by learning from mistakes at the front end, as well as enhancing matching in foreign languages by taking a less linear approach; third, we see more automation of the research inherent in the due diligence process," he said. "This doesn't replace staff, but increases the speed of decision making."

But AI take-up may be slow until both regulators and the industry are more familiar with it. In a poll, more than four in ten of the session audience said complexity and expertise issues would prevent their use of new technologies in compliance, while panellists flagged concerns over model validation by regulators.

Lawlor said the US Office of Foreign Assets Control did not take a prescriptive approach to the methods used to comply with sanctions policy, but nevertheless recommended that technology should maintain a supporting role. "I can see

"Sanctions compliance is turning more into an AML model. The two disciplines are merging.

Lorraine Lawlor, Wells Fargo

how some questions could be answered by machines, but I'm not sure I'd want to rely on one to make a decision on a highly complex transaction."

Industry initiative

Alongside the technologies that individual banks might deploy to improve compliance effectiveness and efficiency, collaborative initiatives were also discussed. In 'Fraud and cyber high alert', panellists favoured industry-led measures, such as SWIFT's Customer Support Programme, over regulatory responses to new threats.

"I view CSP as a bilateral system that allows counterparties to evaluate each other. It empowers organisations to think about their counterparties and their risks," said Jerry Perullo, chief information security officer at Intercontinental Exchange, Inc.

"Initiative has to come from the industry," added James Freis, chief compliance officer at Deutsche Börse Group. "Regulators should be asking firms about the steps they are taking, but if they become prescriptive in their requirements, we become too focused on checking boxes."

A further example of industry-based approaches to protecting banks and their clients is the work of the Wolfsberg Group. Having recently updated the group's correspondent banking due diligence questionnaire in response to evolving regulatory expectations and industry practice, three representatives participated in a dedicated session.

Tracy Paradise, executive secretary of the Wolfsberg Group, said the new questionnaire had been de-duplicated, revised and rationalised. "But the fundamentals haven't changed. The questionnaire sets a standard for the kind of information that banks need to obtain to undertake risk assessments."

Further, panellists hoped that the Wolfsberg Group's effort to standardise due diligence processes between correspondent banks would be of value beyond its current membership and their counterparties. "We've set out the benefits of consistent standards to utilities. If utilities adopt the questionnaire, that will contribute to reducing costs," said Paradise.

> **If utilities adopt the Wolfsberg questionnaire, that will contribute to reducing costs.**
>
> **Tracy Paradise,** Wolfsberg Group

Beyond compliance

The industry's ambition to be effective beyond compliance in the fight against financial crime was also evident in the session, 'AML and assurance'. Ostensibly focused on the role of regtech, the discussion also reiterated the need to recruit and support skilled staff.

Patricia Sullivan, head of financial crime compliance in Europe and the Americas for Standard Chartered, said her bank was trialling machine-learning tools to accelerate repetitive information-gathering tasks, thus freeing up more time for analysis. But she also noted the need for staff to develop new skills, for example to trace cyber-enabled crime proceeds. "Hiring for that skill set – e.g. knowing how to understand digital identification, mapping bitcoin back into fiat currency – is very challenging, although we have had success hiring from the military," she said.

Although technology can reduce both false positives and administrative burdens, Sullivan suggested these efficiencies were secondary to the improvements in effectiveness that would be achieved through a clearer understanding of law enforcement priorities.

The desire to go beyond compliance was palpable from the first session to the last. As Clearstream's Gem observed: "We remain far too quick to rely on a thin veneer of legality to demonstrate that a given high-value transaction is perfectly ok, when your mother would tell you it is not. As long as we continue to define obligations narrowly and systemically, and ignore larger intent, we will continue to fail." ■