

COMPLIANT IS NOT THE SAME AS EFFECTIVE: RETHINKING THE FINANCIAL CRIME PROGRAMME

Financial Crime Studio - Zurich, 24 September 2026. In conversation with Sine Edal, Global Head of Professional Services, IMTF. Written by Oonagh van den Berg, CEO, Virtual Risk Solutions.

A financial crime programme can tick every regulatory box and still miss the risk sitting in front of it. That was the thread running through Sine Edal's conversation at the Financial Crime Studio in Zurich: the difference between a programme that is compliant and one that is actually effective. Sine should know - IMTF's Global Head of Professional Services has spent almost twenty years as a financial crime specialist, and she has watched the industry drift into the first while believing it had built the second.

Investigative thinking beats checkbox compliance

Her answer to what separates the two came without hesitation: the quality of thinking. Checkbox work has its place - consistency, auditability, being able to show the regulator what was done - but it is the floor, not the finish line.

"Check the box does not necessarily mean bad compliance. It means we have to do it - we have to have consistency, we have to have auditability. But it



is not just about meeting your thresholds every day of closing X amount of alerts. It is really getting you to thinking: is there something here that I'm missing?" - Sine

Oonagh took the point further with a metric she treats as a warning sign in itself: KPIs built around closing alerts. Measure people on closure and you incentivise superficial processing - the alerts get cleared, the MI glows green, and the fires keep burning underneath. Worse, the analysts who do the thorough investigations can end up punished for missing their numbers.

"The minute that I see KPIs around closure of alerts, I know immediately that there's going to be a risk involved - because people are incentivized to hit the number. They are not incentivized to do the thorough investigation." - Oonagh

The pair cited a Singapore enforcement action where an analyst stopped one level short of seeing the connections - and the open question of whether the cause was training or the pressure to close. Their money is on the pressure. With FATF's fifth round of mutual evaluations putting effectiveness at the centre, the test for any programme is no longer what the policy says but whether the controls do what they say on the tin: were the inherent risks correctly identified, prioritised, mitigated within appetite - and do the controls adapt as the risk environment shifts? A policy, as one of them put it, is the sprinkles on top of the control framework, not the cake.

Use the intelligence you already have

Institutions, the conversation turned next, are swimming in data they do not use intelligently. Banks hold behavioural data that social media companies crave - how customers spend, where, how often, how their appetites change - yet it is rarely connected up, for risk or for the customer. The answer is not automation for its own sake: automating a bad process on bad data just re-feeds the problem at greater scale. The value is in AI spotting the connections and trends humans would miss - an alert between accounts A and B means little until you follow the money to C, D, E, and F, and a network appears.

Oonagh gave a case from her own alert-review days: money moving between related accounts inside one institution, each transfer with a plausible justification - until the pattern resolved into a human trafficking operation run through a massage parlour. Every step sat in the bank's own books; only the connections revealed it.

Criminals benefit from our silos

AML, fraud, and sanctions teams routinely see fragments of the same picture - and fragmented information is exactly what criminals exploit. Sine argued for breaking the silos down, while acknowledging the obstacles are real: jurisdictions, regulations that sit on top of each other rather than aligning, policies that differ by team - and in Switzerland, banking secrecy, which in some cases forbids teams from talking to each other at all. Oonagh noted the carve-out she had pushed for at a conference - the risk-management circumvention that became Article 75. But both were careful about what breaking silos must not mean: flattening the distinct skill sets each discipline needs.

"Grouping together money laundering and terrorist financing is the biggest mistake we have made in the fight against terrorist financing. Terrorist financing is reverse money laundering - most of the sources are completely legitimate." - Oonagh

Oonagh noted that FATF is now driving the same separation, yet institutions still run one rulebook, built on yesterday's risks, across two fundamentally different threats.

Psychological security, and permission to get it wrong

The conversation closed on culture. Innovation in financial crime prevention needs room to be wrong - false positives tolerated, mistakes owned collectively rather than pinned on a scapegoat.

"What separates the top 1% of companies in the world is psychological security - being able to make mistakes and know that it is collective ownership, not individual accountability. If we want successful innovation, we need the right blend of teams, healthy challenge, and the ability to make mistakes." - Sine

The threat, meanwhile, has industrialised: scam centres that were huts before COVID are now entire compounds; fraud has in many ways become simpler but more psychological - like the letters, indistinguishable from a bank's own, carrying a replacement card and a QR code that empties the account of anyone who scans to 'activate' it. Against that, defenders need data analysts and engineers sitting inside compliance teams, and the confidence to follow a gut feeling before the evidence is complete.

The one piece of advice

Sine's closing advice to every financial crime professional was about people, not systems:

"Use your network - build new networks. Go to events where you meet people from insurance, from technology, from industries and geographies you don't already know. You'll know what trends they're seeing, and you'll know what to look out for in all the masses of data that technology returns to your desk." - Sine

Oonagh's own addition: the biggest asset in her career has been exactly that - being able to pick up the phone to professionals facing the same challenges. We are, as she put it, a global community of people trying to do the right thing. Use it.

