

AML: just comply or ROI?

Anti-money laundering (AML) is a high priority, but if they were being completely honest most executives would probably say that they would adopt whatever minimum standard they needed to get them 'a tick in the box'. To discuss AML compliance further, *Business Management* spoke with Andy Morris, EMEA Risk and Compliance Manager for the Risk Solutions Group at Carreker Limited.

BM Do you find that your bank clients are placing a high priority on AML compliance?

AM. We would say there is a clear distinction between basic compliance and risk management. Banks make investments in compliance because they have to. Investments in risk management are based upon loss prevention and a return on investment. AML purchases normally are not viewed by banks as delivering ROI, but are seen more as an insurance policy should a money launderer target the bank.

When assessing AML compliance, banks usually fall into two categories: those that will invest because they believe that prevention is better than cure and those that believe it will never happen at their bank. Many banks have moved AML into compliance and away from their fraud prevention and financial crime departments. They would probably prioritise AML in the following order, starting with the most important:

- Tactical fraud prevention against specific channels or modus operandi.
- Basel II (credit risk where the bank can measure some tangible benefit from the analysis of its metrics, not full Basel II compliance because no one knows what the benchmarks will be).
- AML compliance.

BM. What is driving banks to invest in new AML technology/solutions?

AM. Regulatory pressures remain the main impetus for banks to invest in AML technology. There is the Patriot Act, the third European Money Laundering Directive, the FATF 40 money laundering and eight terrorist recommendations, Basel II and so on. But the challenge facing banks is that regulations vary around the world. They range from self-regulation by the financial sector ('a risk based approach') to strict enforcement by regulatory agencies where the financial community got it wrong. The threat of fines or, more seriously, of revoking a banking license encourages banks to seek protection against money laundering through both technological investments and properly trained personnel.

Additionally, when banks see other financial institutions receiving fines from US\$3 million up to US\$25 million, or being given a short timeframe to improve AML procedures or face stiff penalties, everybody has to pay attention.

BM. AML concerns are not new, although terrorist concerns have stepped up the pressure. Didn't a lot of banks make AML investments some time ago?

AM. Yes, many did, and for a number of reasons not all were successes – mainly because vendors and buyers alike rushed their decision-making. Installations have failed because expectations were misaligned from the start. Sales were made against regulatory pressure,



When **assessing** AML compliance, banks usually fall into two categories: those that will **invest** because they believe that **prevention** is better than **cure** and those that believe it will **never** happen at their bank



minimising the banks' ability to make prudent investment decisions, articulate requirements or assess whether essential data was available.

Let's be clear: expert systems work if they have all the essential ingredients to make them work, coupled with a well-trained, competent workforce. But there is no one-size-fits-all solution. Each bank has a slightly different customer base from the next. One thing to keep in mind is that while expert systems crunch numbers, humans are required to analyse and act on the data. Expert systems can be badly tuned and maintained. Humans can make bad decisions – a combination of the two is a recipe for disaster. Banks that rushed (or were rushed) into these decisions now have cause to regret, and a reason to reconsider, their AML investment.

BM. What are you advocating as a better approach to resolving AML concerns?

AM. Firstly, legislation needs to change. There is an argument that the industry needs clear guidance and that expert systems are 'mandatory', not just 'best standard practice'.

Secondly, regulators need a better awareness of vendors and their products. Vendors should be certified that they have the 'capability' to meet the local anti-money laundering requirements. Regulators should have a good understanding of each vendor's product so they can enforce (examine) each institution, establishing common benchmarks that are not based upon the subjective analysis of disclosures filed by bank X versus bank Y.

Thirdly, there needs to be a joint effort among bankers, regulators and agencies to openly share information on money laundering trends, best practices and the long-term outlook. Feedback is vital if expert systems are going to be correctly tuned. The vendor also has a role to play here in the form of user groups.

I have seen money laundering and terrorist financing legislation come and go since 1986. After nearly 20 years, we should all be demanding more success, especially in light of the terrorist threat. It's time for individual groups to come together and agree on a mutually acceptable solution.



The decision-maker should explore the potential for his or her investment to be re-purposed in the form of better information, better customer service, better processes and better use of data



BM. Why would anyone – banker or otherwise – object to the approach you describe?

AM. Firstly, mandatory means mandatory and there would be no scope for 'sitting on the fence' or hiding behind the interpretation of best standard practice. However, timing and costs are the factors that will make the proposition unattractive for those banks that have not yet made an investment decision.

Empowering regulators with the knowledge to benchmark and test expert systems should not be threatening for banks that have kept their systems tuned and updated.

BM. What would be your best advice for the immediate future for a bank executive considering investing in an AML solution?

AM. My advice would be to act as soon as possible, but evaluate as many vendors as you can. Don't adopt a 'me too' strategy. Remember that you are purchasing an AML system for your individual bank and one that should not only meet minimum

standards, but that will provide the best protection of your institution from advanced money laundering and terrorist financing schemes. It should also be intuitive enough for employees to comprehend and utilise.

Go with a vendor that has a track record and provides you with the capability to deliver tangible benefits. There is no ROI for compliance; it is an opportunity cost where the bank is weighing the probability of being fined or having its license revoked versus a software purchase.

The decision-maker should explore the potential for his or her investment to be re-purposed in the form of better information, better customer service, better processes and better use of data. This requires initiative and foresight on the part of the banker to ensure that their AML purchase can support the suspension and release of funds in a real-time age and/or analysis of static non-monetary data.

Don't forget that technology is only part of the puzzle. The bank also needs to invest in well-trained staff that has the ability to properly monitor and leverage the system. ■