

Compliance through innovative technology-third party risk management

New technology can make the world a smaller and better-connected place, but one that is potentially more vulnerable to financial crime. Katerina Pagoni describes the manifold advantages of using a third- party dependent operating model to help combat this risk.

In the wake of the Financial Action Task Force (FATF) Mutual Evaluation of the UAE in 2019, banks in the country are eagerly waiting for the results to be published later this year. This may constitute a key driver of any changes that the regulators will require from the financial services industry and of any resultant remediation programmes that banks will need to instigate. Considering that assessment of the effectiveness of the banks' anti-money laundering programmes was in the spotlight during the Mutual Evaluation,

it is probably safe to assume that innovative technology, as a potential enabler of efficiency, will be at the top of banks' strategy agendas.

Criminals can thrive in conditions of uncertainty. They may be quick to exploit windows of opportunity presented by inconsistent application of changing regulations, automation, and innovation programmes that are still in a pilot phase, as well as workforces that are yet to reach the required level of competency.







The imperative for an innovative operating framework

The burden is likely to fall on the banks to define a new operating model that is agile and streamlined, can adapt to emerging financial crime risks and perpetual regulatory change, and leverage technology advances.

In their effort to keep up with the pace of expected regulatory change and technological advancement, many banks are turning to third parties to facilitate technology implementation and inform their business strategy in a cost and scale-efficient way. The possible benefits gained from adopting such an approach can be multiple: it may decrease costs, enhance the customer experience, hasten speed-to-market and augment their competitive edge. Through the integration of bank-held customer data with the data on publicly

available sources, a system that is enabled by artificial intelligence (AI) can employ the same cognitive process to evaluate content as a researcher – without the constraints of human-based research.

Banks are often at varying stages of consideration or implementation of financial-services solutions. Some suggested areas of focus where technology may improve effectiveness and reduce potential human error can include:

- Know Your Customer (KYC) and Customer Due Diligence (CDD) services: despite being a core anti-money laundering requirement and an area of significant investment by many banks, poor execution can be a reality for many organizations. This can result in costly remediation programs, regulatory fines, a detriment to customer experience and reputational damage

- Sanctions compliance: existing screening systems often result in the production of large volumes of false positive alerts and require constant updating due to evolving sanctions regimes, particularly in the Middle East region, and the increasing number of payments and customers. This may translate to a high headcount for the bank and longer transaction times for the customer
- Anti-money laundering transaction monitoring: the regulators are increasingly focusing on banks' transaction monitoring controls as these are key in preventing, detecting and responding to potentially suspicious transactions.

Three lines of defense

Opening the door to third parties, however, may come at a price. There could be a need to implement a robust third-party risk management program for adequate oversight of the relationship and monitoring of third-party risks. These may entail reputation risk, data loss, customer privacy violations, sanctions breaches and poor execution of KYC and Customer Due Diligence (CDD) requirements.

In order to best prevent, detect and respond to such risks, banks could consider establishing a comprehensive financial-services framework constructed in accordance with the 'three lines of defense' principle. It should aim to help organizations identify:

- a) factors that should be taken into consideration to address potential third-party risks
- b) processes that would be required to mitigate these risks during the entire third-party relationship lifecycle.

The additional processes and internal controls required for onboarding and managing third-party relationships could be integrated in the existing framework of the first line of defense. The requirements for oversight and monitoring of the new risks posed by these relationships is likely to come under the remit of the second and third lines of defense.

By turning to third parties for innovative and automated solutions to meet their compliance responsibilities, strategic objectives and customer demand, banks could bear a financial cost. Nonetheless, this could be offset by the multiple rewards they stand to reap after such implementation, such as:

- **Customer:** enhanced customer experience through implementation of the latest technology solutions and automation, which accelerate the KYC and CDD processes, and meet customer demand for:
 - a) access to products and services;
 - b) enhanced protection of their data and privacy
- **People:** people transformation through the upskilling of resources, who will be equipped to work at an organization that is likely to be better positioned for success
- **Process:** likely to have faster, cheaper, scalable and smart financial crime compliance processes that fulfil regulatory anti-money laundering and that can combat the financing of terrorism requirements, can administer large volumes of data at minimum effort and employ artificial intelligence technology that could replicate human analysis
- **Systems:** innovative applications that:
 - a) require less time from the first line of defense to conduct KYC and CDD processes whilst allowing for increased focus on business development;
 - b) enable the second and third lines of defense to reduce the time spent on fire-fighting and instead adopt a more proactive approach in identifying hotspots and potentially preventing issues before they occur.

Navigating the challenges

The likelihood of a successful outcome of the use of third-party innovative solutions for mitigating financial crime risk could be measured by the implementation of a third-party risk management program. This can provide banks with the requisite governance and

internal controls framework and an understanding that by onboarding the third party's solution, the organization is not exposed to a level of risk that is incommensurate with its risk profile. It would therefore benefit from the arrangement through:

- Innovation and technology transformation, but likely not at the cost of increasing financial crime risks
- Compliance with regulations on anti-money laundering and combating the financing of terrorism, without hindering business strategy, growth and competitive edge
- Consistent risk-based approach to risk assessment and due diligence of third parties prior to executing contracts and for ongoing monitoring of the relationship.

Many banks are struggling with both the rate of change within the financial services industry and the global interconnectivity afforded by technology. In such an environment, adopting third-party innovative solutions is an option for banks to meet their multiple targets with regulators, shareholders and customers. Being at the forefront of the global effort to uphold the integrity of the financial system, banks tend to look to innovative technology to best assist them in keeping the perpetrators of fraud and financial crime at bay which may, in turn, prove a worthy enabler.

Katerina Pagoni
Director
Forensics
KPMG Lower Gulf

