Anti-Financial Crime:
A Task for Management and IT

PUBLI-INTERVIEW

actico
Smarter Decisions

Preventing financial crime does not always fall under regulatory specifications. Financial institutions need to protect their clients and themselves.

Sven Feddersen,
Sven is a Project Director at ACTICO GmbH in Immenstaad, Germany. He assists financial institutions in the implementation process of compliance and client management systems. He is the contact person for topics around anti-money laundering, market abuse, embargo monitoring and other regulatory issues.

In your opinion, how well are Swiss financial institutions equipped against financial crime, and what are the greatest challenges?
We see great differences as some technical disciplines are much more established than others. For example, "Money laundering": by now this subject has a lot of history. Within the parties involved (institutes, audit firm, supervision) there are empirical values and some consent for the appropriate processes and measures, so banks are well-positioned in this topic. In the scenario of an IT solution already implemented, questions regarding updates should be carefully considered as there are limits around the amount of data and complexity of tests in introduced systems.
It is a different story for many other criminal acts against the bank itself or their clients, where no comparable regulatory pressures have ever existed. Here mapped out solutions are fewer, and uncertainty regarding the proper approach is greater.

What are the standard requirements that need to be covered by financial crime solutions? In which areas do you see additional need for investments?
A good software solution has to be flexible enough to fulfill the individual needs of the institute. This is especially true during the introduction of the system – for example, defining monitoring scenarios or customizing – where risks specific to the business are the foundation for installing the system. However, high flexibility is still required to adapt quickly to changing situations and requirements. Audit and evaluation logic must be independent from the institution's usual IT release and launch cycle.
In our opinion, the biggest investment needed is implementing preventative solutions. Unlike classic monitoring, which produces some kind of "electronic audit trail" to actively defend against criminal actions, you need to intervene in the bank's operational process and IT systems. That comes with efforts and costs, though.

Will there be more anti-financial crime solutions arising from the cloud?
We recognize a big concern from our customers, despite the higher cost pressure. Many functions cannot be provided readily as a service in the cloud. Problems occur with application scenarios where you want to transmit wide-ranging or sensitive data to the service provider. If there is a lot of historical data to analyze and transmit, necessary updates in the cloud will be required. And even a simple evaluation of personal data and relevant lists, such as PEPs, in a cloud solution means that information about a bank's potential customer is being transmitted to an external service provider. This is always a concern that must be taken into consideration by an institution.

Opportunities for commercial cloud solutions are more likely found in specialized fields, where findings from quantitative and anonymous data can be generated, although these numbers are rather limited.

Source: Interview with SCHWEIZERBANK the leading magazine for the financial industry in Switzerland

However, we expect enhanced cooperation among financial institutions within “community clouds” through an active exchange of usable technical data, such as fraud prevention. It is not cost optimization that will be the main focus, but the possibility for better solutions through the use of information in the network. A prerequisite, however, is legal clarification of data protection issues.

What should banks do to strengthen risk awareness and meet compliance requirements in a timely manner?

Compliance is not fulfilled by IT systems in the company. While IT systems can provide additional information and ensure rules are compliant through automation, using these technical opportunities is only one puzzle piece of all the measurements needed to ensure compliance and defend against criminal activity. Equally important is to define and update the necessary processes, as well as create instructions and practical manuals for daily work.
To create trust with an individual employee, you essentially need a credible and firm commitment to your own policies at all levels of management. This can be applied to a sensitive topic, namely the threat of internal economic crime for the company. A lot of crime and claim cases are caused by employees, and possibly in combination with external third parties. Here, it is important to find the right balance: on one hand, there should not be a feeling of distrust and observing; while on the other hand, there have to be clear barriers. Therefore, clarifying the rules and consistent sanctioning in case of violation is needed.

> "Software solutions alone are not sufficient enough to remain compliant and prevent threats of external or internal criminal acts."

What solutions can you offer to support banks?

Our solution portfolio covers a wide range of compliance features. It is modular based and is used by our customers to fulfill their specific needs. We offer equipped modules in the fields of money laundering, insider trading and market abuse, name matching, embargo monitoring and management of conflicting interests. Each module includes an inspection component to identify unusual or high-risk constellations, as well as case processing for the clarification of hits and documentations.
Above all, we offer institutes the possibility of synergy with "duty" to use for business operations. To do this we illustrate customer onboarding where a variety of compliance demands can be derived in terms of money laundering and terrorist financing as well as neighbouring fields, such as "tax compliance". This leads to two important advantages for the bank: Firstly, client onboarding is completed with the greatest efficiency, despite the high complexity of an extensive product portfolio and international customers who each have different requirements. Secondly, you get a complete and high-quality database as a result, which can be used to service customers and expand the business relationship.
In addition to our role as a solution provider, we see ourselves as a universal implementation partner, and therefore we provide the neccessary services in the fields of project management, professional support and technical advice.

> "If risk can be determined with the help of technical support, the same methods can be used to identify opportunities and potentials."

What are your main findings from already completed projects?

Technical solutions should not fall short. In the case of IT applications, which are supposed to ensure compliance and defend against criminal actions, it is in its nature that the underlying business requirements change over time. This varies for several reasons: There are new requirements by the regulators; there are new insights regarding how to fight off crime pattern, or the bank creates a revised estimation of risks. This means the rules change. And it is now the responsibility of business experts, not IT.
Therefore, our solutions are created in such a way that there is no break between the technical definition – for example, monitoring scenario or risk models – and its technical realization. For this purpose, we use graphical rule models, which also can be used by compliance experts, legal or tax departments.

In a nutshell: In your point of view, what is left to say about this topic? What is your personal advice to top management?

Software solutions alone are not enough to be compliant and defend against the threats of internal and external criminal acts. But they make an important and indispensable contribution, coupled with organizational measures and continuous training and awareness of all employees.

One concern is to only look for technical solutions selectively and in response to current external requirements. Often this results in not using or overlooking synergies in the operational business. While technical support can identify risk, it can also identify opportunities and potentials by using the same methods; for example, on the basis of information around the customer. This is the other side of "Know Your Customer".

ACTICO

EMEA
ACTICO GmbH
88090 Immenstaad
Germany

info@actico.com
www.actico.de

Americas
ACTICO Corp.
Chicago, IL 60606
USA

info@actico.com
www.actico.com

Asia & Pacific
ACTICO Pte. Ltd.
Singapore 573943

info@actico.com
www.actico.sg

02/2016