IT-Based Anti-Money Laundering and Anti-Fraud in Banks and Insurance Companies

Added Value through a Holistic GRC Approach

Frank Holzenthal, computer scientist*[1]

Today, a holistic Governance, Risk & Compliance approach (GRC approach) is the adequate response to business challenges in an increasingly interconnected world. IT systems that integrate GRC functions help bank and insurance companies to comply with the numerous statutory, legal, and regulatory requirements, create transparency for business relations, plan and execute measures and controls and make strategic decisions regarding risk and compliance.

1 Challenges for Banks and Insurance Companies

1.1 Anti-Money Laundering and Terrorist Financing

Money laundering introduces illegal assets from drug trafficking, prostitution, illegal gambling, or arms trade into the legal financial and economic circulation by concealing their origin. Globalization has seen the development of methods that are more sophisticated making it increasingly difficult to prevent acts of money laundering. In order to contain organized crime and protect the financial system against misuse, global standards have been developed and numerous laws passed (e.g. EU money-laundering directives, USA Patriot Act, Bank Secrecy Act, FATF 40+9 recommendations) that are being made more rigorous on a regular basis.

Banks and insurance companies are particularly affected by money-laundering risks due to their product portfolio. Anti-money laundering and compliance departments often struggle with the ongoing challenge to protect their organizations against misuse and comply with current statutory requirements. These enterprises are under increasing pressure to completely disclose their business relations and to meet the numerous statutory regulations.

An efficient IT-based check strategy becomes the decisive competitive factor for financial service providers. Apart from compliance with legal requirements, flexibility, low cost and time expenditure are critical factors to maintain and update the money-laundering check procedure.

[1]Frank Holzenthal, computer scientist and member of the management board of TONBELLER AG, Bensheim; contact: fh@tonbeller.com

1.2 Anti-Fraud and Fraud Prevention

Banks and insurance companies are increasingly shifting their focus to the fight against fraud and its prevention. In general, fraud is neither confined to a region or industry nor has it anything to do with the size of the organization. National and international studies, e.g. by the Association of Certified Fraud Examiners (ACFE)[2], show that the damage caused by fraudulent actions poses a serious threat to the economy. Furthermore, numerous legal requirements (e.g. UK Bribery Act, German Banking Act) demand checks to be extended to "other criminal actions". This entails the need to search for fraudulent actions.

Due to criminal creativity, new variants evolve every day for online banking, insurance or internal fraud. Electronic media are increasingly used for criminal actions, since invisible and anonymous money transactions facilitate the concealment of fraud.

Yet, the actual fraud-induced costs reach far beyond the financial loss. Banks and insurance companies are challenged with securing their customer's assets, avoiding own financial disadvantages and long-term damage of their reputation.

The efficient fight against fraud requires software that not only detects fraudulent actions but also helps preventing them in the first place. The imbedded real-time components allow minimal response times with high decision quality and aims at fraudulent activities with a high damage potential.

2 IT Systems for Anti-Money Laundering and Anti-Fraud

2.1 Added Value through Integrated IT Systems and Flexible Standard Software

By combining the fields of Governance, Risk & Compliance, organizations avoid economic or legal damage to their businesses or of their reputation and gain a sustainable competitive edge. By integrating GRC functions with the specialized departments and local business units, IT systems add value for the corporate management.

This integration is critical to success and profitability of compliance systems, since the combination of risk, monitoring and control systems enhances the transparency of the compliance process and thus makes complexity comprehensible. Individual compliance tasks that are handled by isolated systems make it difficult to merge information. Risk interdependencies in the company's divisions that identify and monitor risks independently may not be detected at all in the worst case thereby generating and

[2] http://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf

increasing the potential damage for the company or preventing the recognition of connections that are indicators of financial crime.

Integrated IT systems combine the compliance operation 'silos' into a compact and meaningful system to fight financial crime. The integration grants the necessary transparency and a cross-departmental and cross-organizational coordinated approach. The embedding of compliance systems enhances the range of the risk-management radar by transcending the genuinely operational risks. In combination with risk management, the compliance strait jacket turns into a bulletproof vest. Governance for its part profits from a more solid basis for corporate management. The integration increases the company's profitability and reduces costs through less interference or redundant processes in the departments.

Banks and insurance companies should prefer flexible standardized solutions that can be customized and scaled to fit into the company structure, its processes, IT systems and existing GRC systems. Flexibility is also important at the specialist level. Rigidly implemented solutions are incapable of complying with the risk-based approach stipulated by law. If this approach is used it makes sense to choose a solution that can be adjusted to the company's risk situation without requiring any programming skills. This is achieved through scenario editors that can be used to define recognition patterns based on master data from the customer and account base, on transaction data and on customer profiles.

2.2 IT-Based Anti-Money Laundering

2.2.1 Assess and Manage Money-Laundering Risks

A comprehensive anti-money laundering solution supports the creation and continuous further development of the institution's risk analysis. Identification, categorization, and the assessment of money-laundering risks are the foundation of all subsequent activities that initiate and design anti-money laundering programs. Targeted organizational steps may then be derived and IT prevention measures implemented. This does not only support the individual control of money-laundering risks. Focusing on essential risks may also result in savings through efficient resource allocation and check procedures that are more potent. Integrated workflows for cross-departmental risk assessment, audit-proof documentation, and custom evaluation options should complete the picture of the risk-assessment functionality.

2.2.2 Risk Assessment of New Customers

New customers are risk-assessed using information that has been gathered during the process of customer acceptance. This data should be matched with all available databases. On the one hand, this applies to databases that identify the beneficial owner of a corporate customer. The entire company is to be treated accordingly if one of these beneficial owners poses a high risk. On the other hand, sanctions and PEP lists are to be taken into account by matching them with the customer data (and that of the beneficial owner, if applicable). Sanctioned persons must be rejected as soon as they are trying to initiate a business relation with the institution. Recognized politically exposed persons (PEPs) are to be considered high-risk customers and treated with enhanced due diligence. Furthermore, applicants are to be classified by assessing their risk based on the information they have provided. To this end, it makes sense to keep the risk-assessment criteria customizable, so that they can be adjusted according to the individual data[3] provided by the new customer.

2.2.3 Risk Assessment of Existing Customers

In contrast to the initial risk assessment of new customers, the risk assessment of existing customers is a continuous process that is to be repeated in regular intervals. Any reclassification must be archived to be audit-proof on demand. To classify the risk of existing customers, significantly more information is available in the research systems than at initial customer assessment, since the customer's transaction behavior, profile and current product use is already known. The integration with the initial risk assessment enables the institution to detect deviations from the behavior specified at customer acceptance and to consider this for the continuous risk assessment.

2.2.4 Detecting Money Laundering Through Customizable Scenarios

After customer acceptance, due diligence[4] applies to each risk-classified customer (e.g. high-risk private customer) while searching for acts of money laundering. The representation of this gradual due diligence needs to be a standard feature in solutions aiming at the detection of money laundering. Furthermore, such a system should also be shipped with a set of specified money-laundering check rules. These are, among others, rules to detect smurfing, dormant account at banks that show sudden activity, the premature cancelation of an insurance policy, frequent changes of the beneficiary or the reclaim of

[3]This individual data consists of master data, compliance-specific data, information on the intended product use and transaction behavior or the goals of the business relation.
[4] According to EU directive 2005/60/EG

excess amounts. Such solutions distinguish themselves through options for Money-Laundering Officers allowing them to specify and describe additional money-laundering scenarios on their own.

Deviations from the initially described behavior may be detected automatically if the customer acceptance process is integrated. An alert is triggered if the customer does not behave accordingly. Integrated case management functionality should support investigation of the alert and the overall decision process from invalidating an alert to filing a suspicious activity report (SAR).

2.2.5 Matching Payments with Sanction Lists

In accordance with international requirements[5], all companies that post transactions are to ensure that they do not support terrorist financing unintentionally. To this end, transactions must be checked in real-time with publicly available[6] sanction lists. In case of matches, the payment must be stopped immediately and presented to the responsible person for a decision. This time-critical process needs to be workflow-based (incl. e-mail notification, user authentication, dual control, etc.). Intelligent systems, however, do not only match with sanction lists but also allow the creation of custom business rules. Such business rules may sharpen the sanction list result, prevent false positives or send e-mail notifications depending on specific data constellations.

2.2.6 Visualization, Management, and Control of Anti-Money Laundering Measures

The active management of money-laundering risks for all connected national and international departments and subsidiaries requires an up-to-date daily and central overview of the most important Key Performance Indicators (KPIs). Through visually appealing cockpits, banks are granted a holistic view on their risk analysis including all preventive measures and their status. Based on consolidated data from integrated risk-assessment and research systems, measures are calculated and presented in a clear and structured manner using sophisticated visualization techniques.

2.3 IT-Based Anti-Fraud and Fraud Prevention

2.3.1 Assess and Manage Fraud Risks

The efficient fight against fraud requires a corporate risk assessment and tools to identify and monitor both known and new complex risks. If the IT-based risk assessment is integrated with the anti-fraud

[5] E.g. EU directives 2580/2001, 881/2002, U.S. Patriot Act, etc.

[6] For instance, the watch list of the European Union, the Office of Foreign Assets Control (OFAC) of the U.S. Treasury Department, the HM treasury (the UK's Economics & Finance Ministry) or the UN resolutions 1267 and 1988 .

research system solid key figures may enrich the risk analysis. The effectiveness of IT prevention measures may then be ascertained automatically and the risk evaluation can be continually refined along with the resulting measures.

2.3.2 Risk Assessment for New and Existing Customers

The risk assessment of new and existing customers regarding potentially fraudulent actions may be seen as an extension to the risk assessment from the anti-money laundering perspective as described under 2.2.2 and 2.2.3. This risk assessment, however, not only uses transaction data and customer profiles but also takes further data and non-monetary events (e.g. frequent address changes, frequent query of specific data, premature canceled contracts) into account. Furthermore, not only the customers need to be classified but also all parties that are involved in the transaction (e.g. banks, recipients or the operating staff).

2.3.3 Protection against Fraud Attempts

In contrast to genuine money-laundering checks, checking other criminal acts is more laborious. Scenarios are not clearly defined and the patterns of fraudulent actions change on an almost daily basis. Cases of fraud are also often complex events that need to be recognized within a tight timely order. A Complex Event Processing solution links events that do not have any apparent connection. If suspicious patterns and sequences are detected a warning is issued, followed by a real-time alert if the threshold is reached that must be decided as soon as possible. Only this procedure allows the prevention or containment of fraudulent actions.

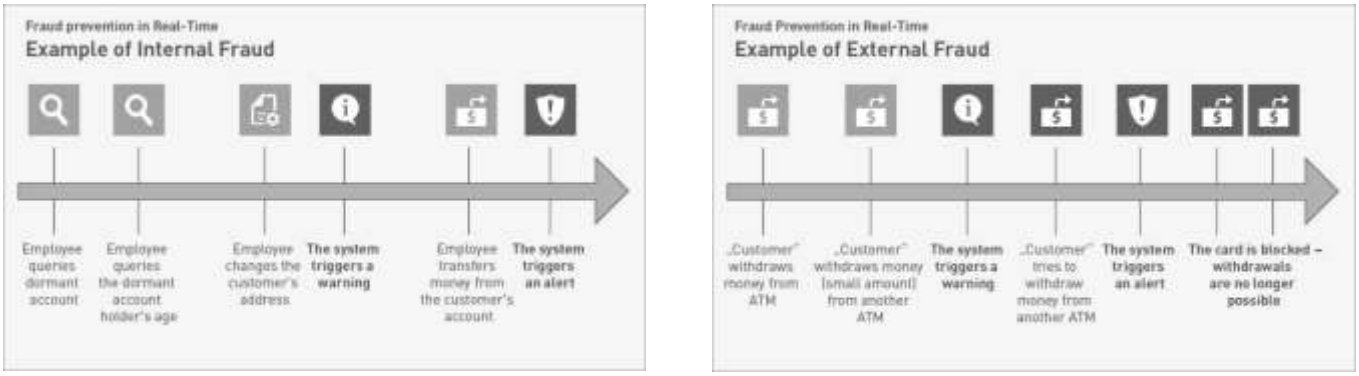

Figure 1: Fraud prevention in real-time

Figure 1 visualizes that:

- *Internal fraud:* An employee often queries an inactive account focusing on the account holder's customer age. Then the customer address is changed so that account statements are no longer sent to the bank's customer. This is where the system steps in to generate an alert. As soon as the employee uses this account for the transfer of money, the system triggers a real-time alert.
- *External fraud:* A small amount is withdrawn from the ATM followed by a withdrawal at a second ATM with the same card shortly after. The system may now already generate an alert, especially if the two ATMs are located in a significance distance from each other. If these withdrawals only serve a testing purpose, the defrauder who succeeded with the previous two tests will try to withdraw larger amounts in short intervals. In this case, the system immediately triggers an alert and blocks the card at the same time.

A Complex Event Processing solution enables banks and insurance companies to react immediately and to specify flexible scenarios. It should be noted that IT-based fraud detection systems must be tightly connected to the banking processes. From the ethical and technical point of view, the staff council and the audit department is to be "taken on board" when implementing such an IT solution, especially if internal fraud is concerned. Sensitive data is to be made anonymous and labeled with pseudonyms. Only in the case of a substantiated suspicion, this data can be deciphered by including a third party (e.g. the audit department).

2.3.4 Visualization, Management, and Control of Anti-Fraud Measures

As with anti-money laundering, it is also essential for the fight against and the prevention of fraud to gain a holistic view on the materialized and the prevented damage and the potential fields of fraud (customers, products, transaction types and countries) to be able to report the key data to the management. This requires dashboards and cockpits.

3 Conclusion

Measures to fight financial and white-collar crime can only be efficient if implemented through an integrative IT approach that combines the fields of Governance, Risk, and Compliance in banks and insurance companies. It is of utmost importance to link all disciplines with each other, from risk analysis and the efficient recognition of, and fight against, dolose actions (fraud, money laundering, terrorist

financing, and others) to the holistic representation and visualization of relevant key figures and magnitudes in an overview.

IT solutions must be suitable for the user with intuitive user interfaces and fast access to the required functionality. The IT department should only be involved during the introductory phase of such a software and for maintenance purposes. Standard software that offers flexibility and models the expert complexity is to be preferred. At the same time, IT systems must be capable of fully integrating with existing processes at banks and insurance companies.