Financial crime compliance
It is no longer sufficient to 'go it alone'

Luc Meurant
Head of banking markets and compliance services
SWIFT

Multiple factors make compliance with financial crime legislation one of the most difficult challenges facing the chief operating officers of banks and other financial institutions today.

First, the penalties applied for non-compliance are steep and only getting steeper, with billions of dollars of fines levied in the last 15 months. More costly still is the remedial expense of improving processes and adding personnel to cope with the increased workload of preventing such action in the future. It is important to note that these costs are not limited to institutions that have been cited for violations; it is safe to say that nearly every financial institution is spending substantially more on financial crime compliance-related activities compared to just a few years ago.

This picture is further complicated by the diverse and constantly evolving nature of financial crime, including the fact that the rules differ across major jurisdictions and are subject to regular change. COOs face the reality that financial crime compliance is much harder to measure than other aspects of operational risk, making it more difficult to define meaningful benchmarks for 'what good looks like'.

The cost of doing business

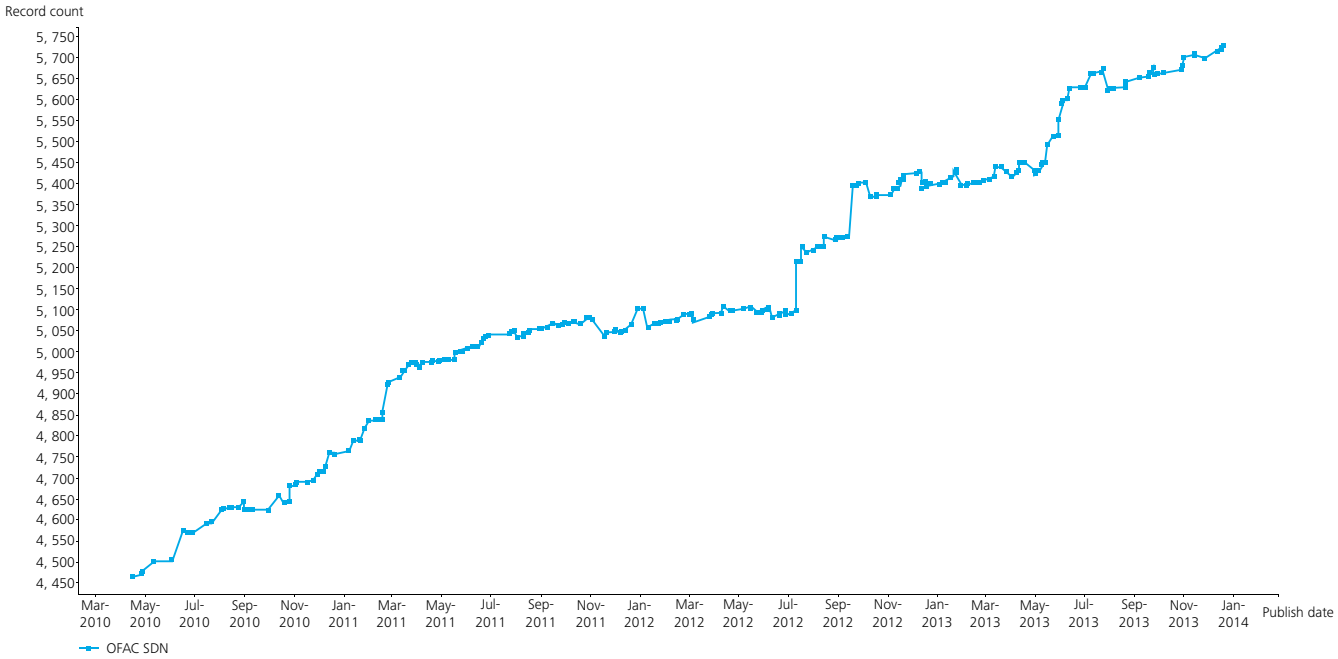
Banks must accept that compliance is an essential pre-requisite of doing business. However, a combination of high stakes, fast-evolving risks and an absence of best practice has resulted in a ballooning of banks' compliance budgets, but with no real certainty of success.

In July 2013, a global survey of 300 senior compliance executives at financial institutions conducted by Veris Consulting found that 57% of respondents had increased their anti-money laundering and Office of Foreign Assets Control (OFAC) compliance budgets in the past 12 months. But almost a third said they still felt their budgets were 'inadequate or severely inadequate'. This is further confirmed by a global survey of financial institutions released in December 2013 by *BAE Systems Applied Intelligence and Operational Risk & Regulation magazine*, which found that half of respondents expected to increase investment in compliance by 20%.

With regulators frequently raising their expectations in terms of sanctions compliance and the definition of non-compliant transactions subject to interpretation, banks must make their own decisions on the investment levels, policies and procedures that must be adopted to avoid falling foul of financial crime legislation.

For example, regulators expect banks to prevent transfers involving individuals cited on a sanctions list, regardless of the many possible ways their name might be represented (even a first name can have many variations, e.g. Bob, Robert, Rob, Bobby, before initials and titles are even considered), which means that each bank must decide how far they should deploy technologies and techniques to comply with sanctions rules.

Figure 1: sanctions list growth - OFAC SDN



Measuring the unmeasurable

In this context, banks' compliance budgets are potentially limitless. Not only does increasingly sophisticated technology need to be applied to screen greater numbers of transactions, but more staff are required to analyse the alerts thrown up by the technology.

Within most areas of banking operations, metrics have been developed to accurately measure effectiveness. But in a low-probability/high-impact area such as financial crime compliance, measuring and optimising effectiveness is far from straightforward. If tighter monitoring policies increase the number of alerts investigated by your sanctions monitoring team from 100 to 120, have you actually reduced the level of compliance risk, or simply increased the team's workload and related operational cost? How do you balance the need for smooth operations and good customer service with the mandate to identify and block all transactions that might be in violation? These unmeasurables mean that the traditional COO challenge of devising strategies to improve operational efficiency, then monitoring and measuring their impact to optimise processes on an ongoing basis, is an imperfect guide to optimising financial crime compliance policies and procedures or to setting compliance budgets.

> Just because your bank's compliance challenges are unique does not mean you must tackle them alone

The role of standardisation

A further difficulty facing COOs is that regulatory supervision in financial crime compliance is evolving more rapidly than most tools and solutions can handle. Automation is essential of course, but it requires continual investment. Over the past decade, increasingly advanced technologies have been introduced to support banks' compliance efforts, but these have often addressed very specific needs, leaving a very fragmented picture from an enterprise-wide perspective. This means that implementation costs typically overwhelm the prices paid for the compliance software itself, with significant resources required to upgrade, inter-connect or replace existing solutions. This also hampers second-level controls, i.e. the systems that check that compliance systems are working properly.

In addition to delivering cost-savings, the move to a more standardised approach would help banks allay regulators' concerns and support both parties' efforts to further establish best practice. The gradual standardisation of financial crime compliance policies and solutions would offer banks the opportunity to take best practice to another level.

As with any new or fast-evolving requirement, banks have tended to initially tackle financial crime compliance in their own individual way, only over time realising the inefficiencies of ploughing investment into solving essentially the same industry-wide problem. In non-competitive areas, such as compliance with financial crime legislation, this stage should come sooner rather than later. And it is beyond doubt—as Basel III and other reforms erode banks' balance sheets—that financial crime has reached the point where the need for standardised practices at lower cost brings forth the case for shifting from proprietary solutions to utility approaches.

The move to collaborative solutions

The realisation that financial crime compliance budgets could be a bottomless pit has motivated banks to move from standalone investments to a more long-term approach, where collaboration helps the industry benchmark its compliance efforts and mutualise their cost.

Many of the benefits of the utility approach have been established in related fields of banking operations. A dedicated industry-wide utility can help to capture and define best practice and serve as a forum for further innovation, as has been seen in the evolution of message standards for example.

One area of interest to SWIFT users is that of Know Your Customer (KYC) compliance, where a number of our member banks have explicitly called for us to develop a KYC utility to help tackle this compliance burden in addition to the sanctions solutions we already offer.

Ongoing KYC compliance involves demonstrating that you have access to the relevant information about your clients, that you have put the necessary due diligence processes in place and that you have performed the necessary validation and analysis to determine the level of risk related to each counterparty.

Although KYC compliance has its most visible impact at the onboarding stage, this is just the beginning for banks, as information must be kept up-to-date and stored so it can be integrated with other sources of data within internal systems and shared with other banks when necessary. The diversity and frequency of KYC requests from third parties (where the same information may be required multiple times) means that the quality of data and data management processes are critical for efficient KYC compliance. All too often however, information requests are handled on an ad hoc—and at least partially manual—basis.

A further consideration is whether to concentrate KYC compliance so that all business units and branches follow a single centralised policy or take an approach based on meeting the differing requirements of local regulators. When you consider the difficulty in verifying that the information supplied is both accurate and up-to-date, the need to rationalise, standardise and streamline the current plethora of KYC requests and processes becomes apparent. What is more, many of the jurisdictions across which most banks operate are regularly raising the bar, tightening and tweaking policies at a rate that forces banks to develop long-term systems and solutions which enable them to adapt to the ever-moving target that is KYC compliance.

KYC utility—prerequisites for success

The existence of a central hub to which a bank would only be required to send any single piece of information once—instead of today's infinite number of times—would represent a significant efficiency gain for the industry. As such, SWIFT is creating a KYC registry which will help users reduce the cost, effort and risk related to KYC compliance, including tracking the validity of documents, sending reminders if documents expire and providing notifications if updated information becomes available.

For any utility solution to be successful, several elements must be present. First, there must be an acceptance of the need for a cooperative approach among key stakeholders. Second, the utility operator must be able to create standards on which best practice can be established and innovation can flourish. Third, the utility must achieve and maintain high standards of operational excellence on which its member banks can rely. Finally, the utility must have access to the necessary skills and expertise in the field for which it wishes to provide a service.

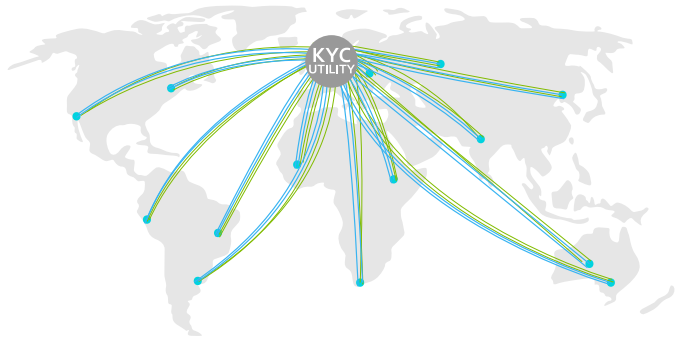
Compliance will always remain the responsibility of the bank and so all utilities must be transparent in their processes and policies. This is why SWIFT's KYC registry has established a working group of member banks responsible for validating the scope of the initiative, formalising the required functionality and, over time, encouraging participation across the wider banking community.

Ultimately of course, a utility is only a means to an end, helping individual banks meet their compliance obligations to their particular regulators by demonstrating the effectiveness and appropriateness of their processes and the systems they have put in place.

Figure 2: KYC registry

Now

Future



The realisation that financial crime compliance budgets could be a bottomless pit has motivated banks to move from standalone investments to a more long-term approach, where collaboration helps the industry benchmark its compliance efforts and mutualise their cost

The drive toward continuous improvement

The challenge for banks is to move toward a point at which their financial crime compliance measures are repeatable, predictable and aligned to their risk profile. If banks can achieve this objective, they will be better able to measure and therefore continually improve the effectiveness and efficiency of their compliance strategies. Given that continuous improvement is essential, the number of transactions requiring monitoring and the number of risks is only going to increase. If COOs are to bring their spending on financial crime compliance under control, then measuring, benchmarking and sharing best practices are essential. We believe utility solutions can and will play a key role in this area.

In summary, we sense a shift in the industry's approach to compliance, from KYC to sanctions.

We believe banks are now more willing to share, talk and be more transparent in areas where it is in their collective interest to work together on joint initiatives. Financial crime compliance is just one such area.

In addition, we believe standardised solutions will unlock economies of scale. SWIFT's Sanctions Screening product serves as a good example. Although implemented slightly differently in each instance, the same product is being used in almost 70 different countries.

This demonstrates that many of the needs of banks in complying with financial crime legislation are common and can be tackled through solutions built on standards. Just because your bank's compliance challenges are unique does not mean you must tackle them alone.

Reliable AML controls based on complete and accurate static data

An ongoing challenge for professionals

Michael JJ Martin
Partner
Enterprise Risk Services-
Forensic Services Risk,
Compliance, Attest
Deloitte

Nicolas Marinier
Senior Manager
Enterprise Risk Services-
Forensic Services Risk,
Compliance, Attest
Deloitte

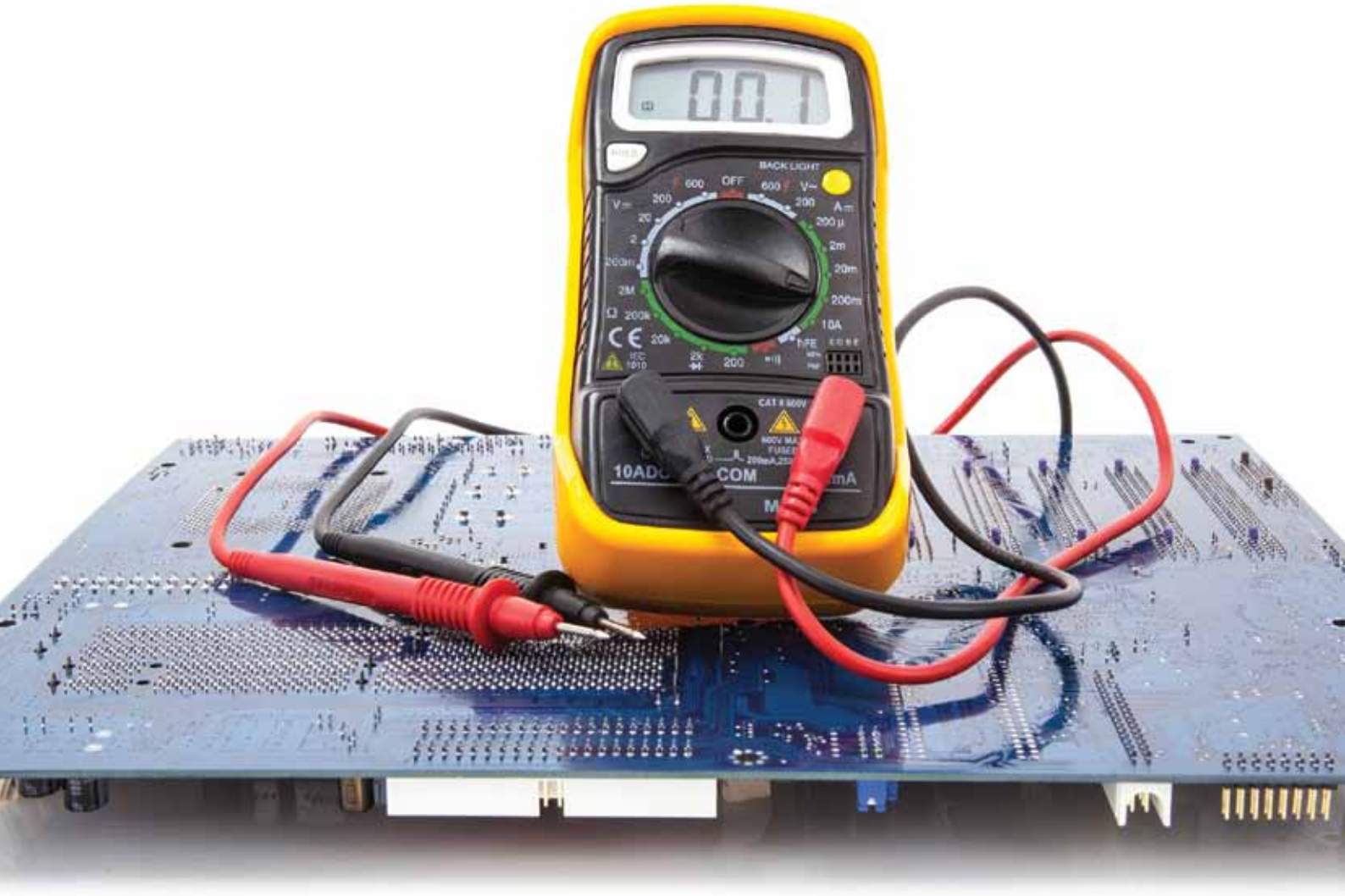
Context

In recent months, many articles have been published by the international press about suspected cases of money laundering. The media continue to report on a wide variety of money laundering scandals.

Sanctions have also reached unprecedented heights with a record fine of USD 1.9 billion paid by an international bank in December 2012 to settle allegations of Mexican drug traffickers and terrorists using this bank to move money around the financial system.

The risks of money laundering and terrorist financing continue to top financial and political agendas and these risks fall under the scope of both internal and external audits for the financial sector. As the money laundering and terrorist financing risks encountered by professionals have evolved, the legal and regulatory framework has quickly been adapted, given increasing pressure from regulators worldwide to have professionals revise and update their controls and systems in order to fulfil their professional obligations.

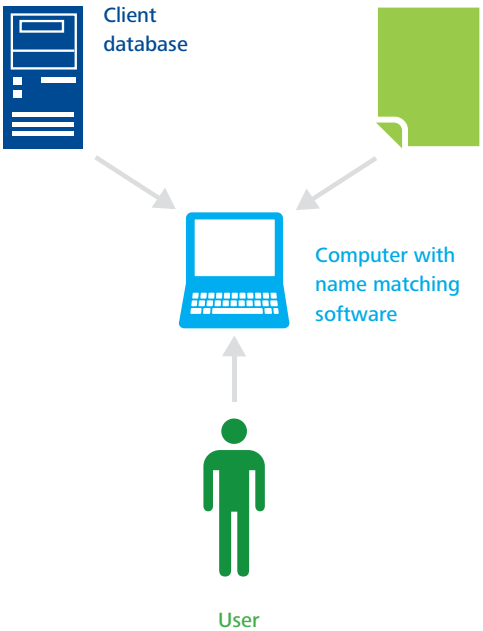
Money laundering and terrorist financing are dynamic and continually evolving phenomena that demand the vigilance of professionals, who must keep abreast of the latest developments and trends



Importance of static data and background information

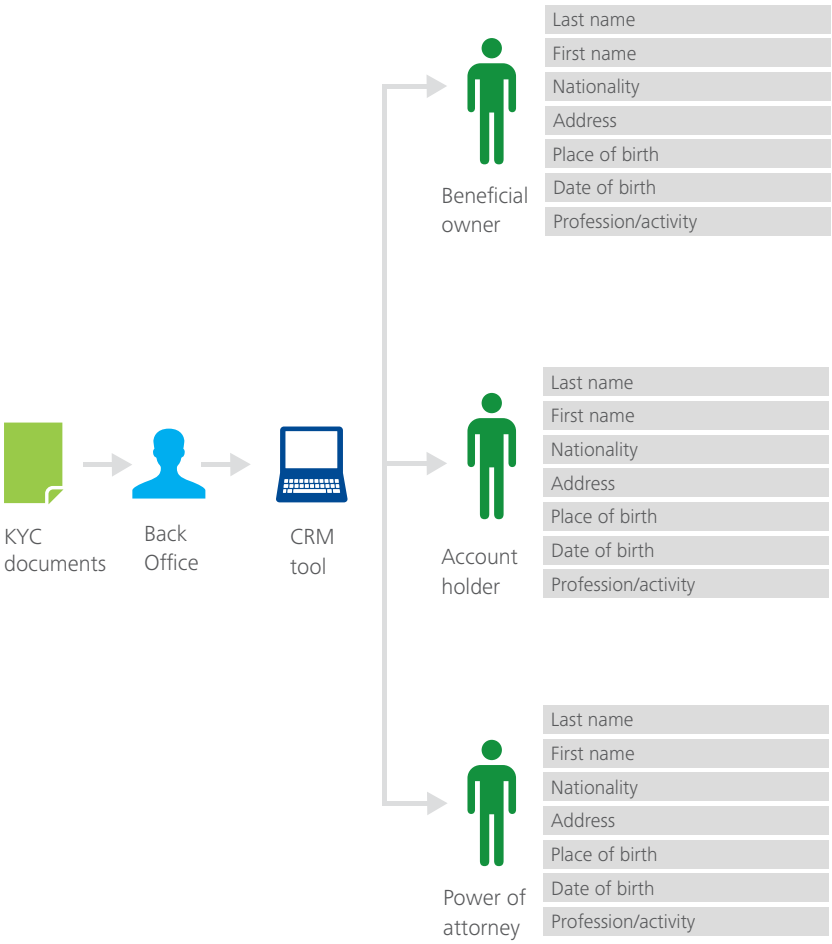
In light of the risks and challenges mentioned above, it is critical to have complete and high-quality static data, which are the raw material used for risk rating and related mitigating controls. Risk rating takes the clients' various characteristics into consideration (country, type of client, activity/industry, PEP (politically exposed person) status, non-face-to-face, etc.) as well as the type of services provided (nature, exposure, underlying assets, distribution channels, etc.) and attaches a weight to each criterion to calculate a global risk score. This is detailed in CSSF circular 11/519 or 11/529 and in articles 4 and 5 of CSSF regulation no. 12-02.

Based on this risk rating, name screening and transaction monitoring are applied with differentiated frequency. Name screening is performed both on the client database and on the electronic transfers (originators and beneficiaries).



- Blacklists - Criminals and terrorists
  - UN list
  - EU list
  - Luxembourg Public Prosecutor
  - Any other private lists
- Sanction lists
  - OFAC (Office of Foreign Assets Controls)
- PEP lists
  - (CIA)
  - Dow Jones Factiva
  - World Check
  - etc.

For name screening on the client database, all relevant information about the client and other related parties (such as ultimate beneficial owners, directors and authorised signatories) must be correctly and exhaustively entered into the database used for Client Relationship Management ('CRM').



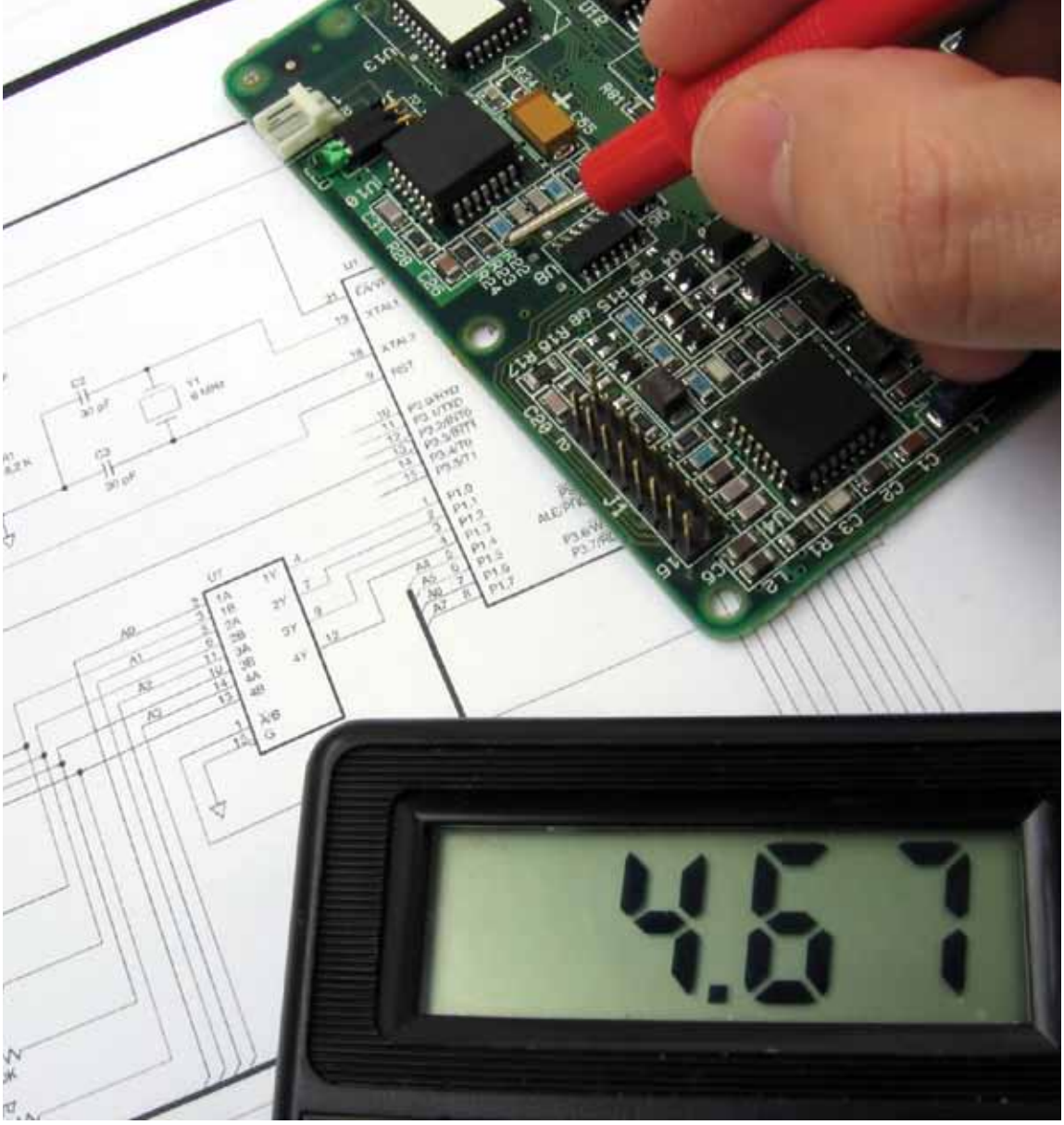
Furthermore, in order to generate useful and reliable queries and statistics, it is essential to ensure that static data is in a consistent and harmonised format. For instance, if nationality data for the United States is inputted as 'U.S.', 'USA', 'United States', 'America', 'California', etc., the quality of controls is severely undermined.

Static data corruption can occur during a Customer Relationship Management system migration given that static data relating to clients/investors and their linked parties may be altered. There is a risk that the names of clients/investors or of the persons linked to corporate accounts may go missing, or even that some clients'/ investors' date of birth may be indicated as 01/01/1900 (the system default date in the case of field format incompatibility).

Human error also regularly represents another hazard for static data. This is the case, for instance, with clients/ investors going through third party introducers, whereby the names, date of birth, nationality or other information about persons linked to corporate accounts may be missing because a third party introducer did not collect this information. As a consequence, alerts may be missed or too many false positives may be generated.

Static data is processed using name matching software that generates alerts for potential hits, which are to be reviewed by the user and classified as true or false positives. This classification is carried out using factual elements used as elements of differentiation to support the decision whether a potential hit is a 'true' or a 'false positive'. A false hit could be justified, for instance, in the case of a different date of birth or middle name. Once more, it becomes apparent that static data completeness and accuracy are critical.

Based on static data from the client and transaction database, the transaction monitoring system processes financial flows using frequency, thresholds and rules and against predefined money laundering detection patterns.



Client data is also used when reviewing the generated alerts to analyse the coherence with the initial account purpose and expected transactions. Here, information on the source of wealth required by article 24 of CSSF regulation no. 12-02 proves valuable, as it provides the professional with a context to corroborate volume, frequency and origin/destination.

As such, ensuring the completeness and quality of static data is the first key step for professionals in order to effectively carry out their procedures and controls.

Remediation

Procedures and controls calling for a degree of diligence are implemented when collecting client data in order to prevent and manage the risks of money laundering and terrorist financing. New accounts are opened based on current procedures in line with up-to-date requirements for complete due diligence and KYC documentation. For existing accounts, there is a risk that information may be missing or outdated.

In light of mentioned risks and challenges, it is critical to have complete and high-quality static data, which are the raw material used for risk rating and related mitigating controls

This risk is often the hardest to remedy, due to significant regulatory changes in recent years and the commercial difficulty associated with requesting additional information from clients in a long-standing relationship.

Remediation usually starts by reviewing the scope definition and analysing any gaps between existing KYC/AML procedures, controls, documentation and current AML professional obligations. Once the gap has been identified, tasks are prioritised in accordance with the risk attached to the incomplete files.

Procedures can first be reviewed to facilitate the analysis of account opening files, using an updated version of procedures in line with current requirements. Often, KYC files identified as 'high risk' and complex structures (offshore companies, trusts, foundations, etc.) are the main area of concern for professionals, as reviewing and remedying any risks associated to them is time consuming and involves a heightened risk of money laundering or terrorist financing.

When account opening files are reviewed, the missing information and documents are collected from relationship managers, intermediaries or clients as part of the remediation effort. The purpose of remediation is to ensure that static data to be stored in the CRM system are complete.

Deficiencies identified during the review can be inputted directly in the professional CRM or in a dedicated review tool with a separate database that will be used during the remediation effort to update the static data.

The lessons learned from file reviewing and remediation assistance exercises show that the main issues are those presented by information and supporting documentation relating to the source of wealth, both for individuals and legal entities as well as the beneficial owner structure for legal entities.

Using knowledge from relationship managers and Open Source Intelligence[1] ('OSINT'), a large proportion of the deficiencies can be solved with no or limited information requests to the client. The information collected can be complemented by a memo with all the available information and all field research, visits or verification that the professional has performed to corroborate the client's explanations.

The upside of such an exercise is that the professionals improve their knowledge of the client, which can be later turned into a commercial opportunity.

Remediation also deals with missing or incomplete name screening and transaction monitoring. Remediation is required for clients for whom no recent name checks have been performed or exception reports were not properly followed up, the latter being the worst-case scenario.

The remediation exercise shows differences in the way the name is spelt, in the first/middle name, country, date of birth, place of birth, country, occupation, etc., thereby supporting a classification as a false hit or leading to a Suspicious Transaction Reporting. In the case of a real hit, the nature of the hit is analysed (PEP, individual, crime, terrorist, etc.) as they do not all have the same impact and consequences. Some might trigger a Suspicious Transaction Report (STR) to the Public Prosecutor. The professional then adds a comment to explain the impact on the risk rating and the relevant action.

1 Open-source intelligence (OSINT) is intelligence collected from publicly available sources.

KYC is still a hot topic

Money laundering and terrorist financing are dynamic and continually evolving phenomena that demand the vigilance of professionals, who must keep abreast of the latest developments and trends. Preventing money laundering and terrorist financing remains a major concern due to the inherent threat it can pose to the integrity of legitimate financial institutions and the financial risk of severe penalties and the legal ramifications it represents. With complete and updated data, however, professionals of the financial sector are better equipped to detect and manage the risks of money laundering and terrorist financing.

The risks of money laundering and terrorist financing continue to top financial and political agendas and these risks fall under the scope of both internal and external audits for the financial sector