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

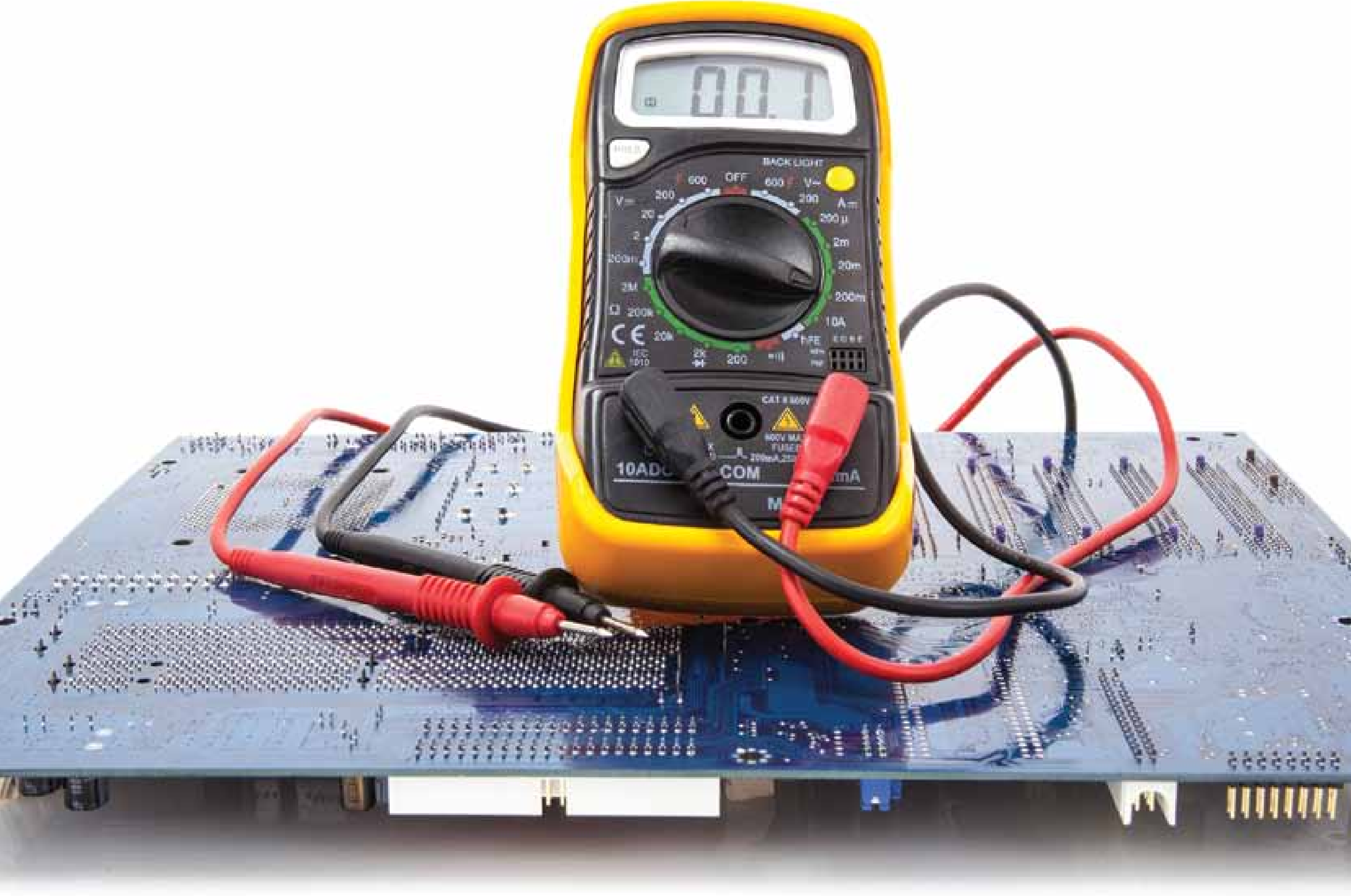
Context

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.

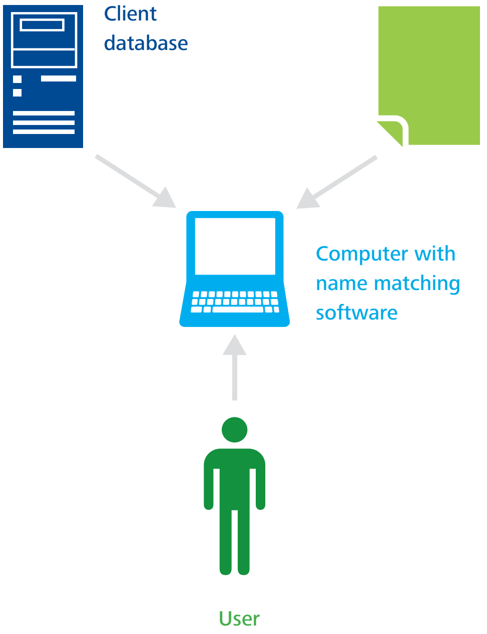
Money laundering and terrorist financing are dynamic and continually evolving phenomena that demand the vigilance of professionals, who must keep abreast of the latest developments and trends



Importance of static data and background information

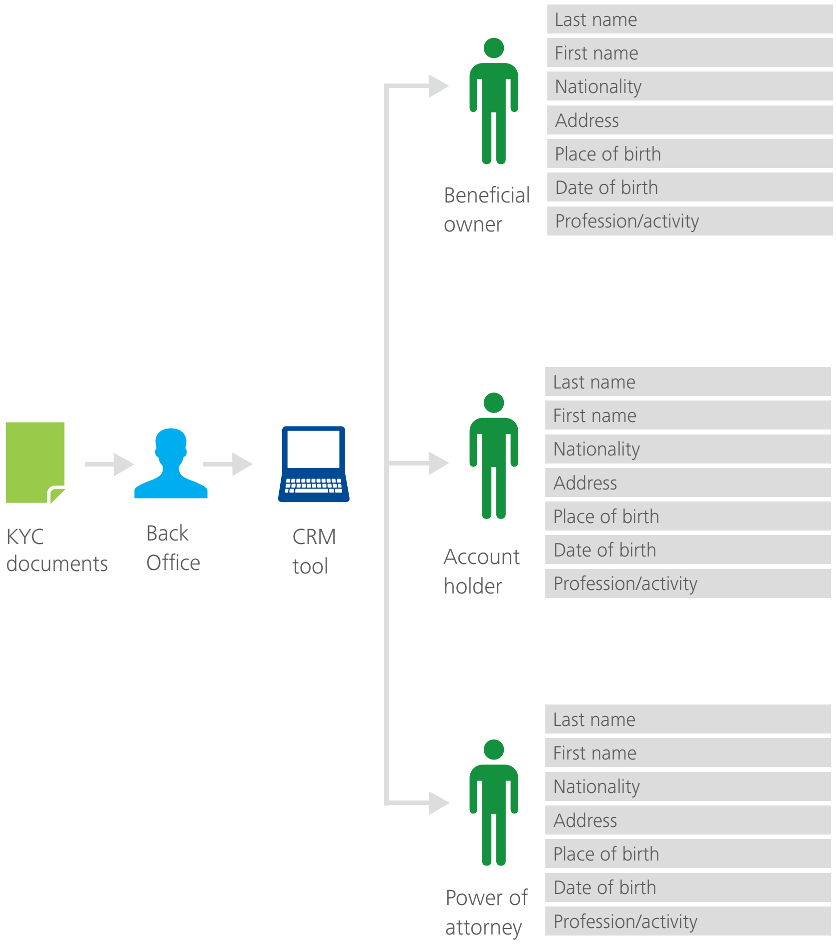
In light of the risks and challenges mentioned above, it is critical to have complete and high-quality static data, which are the raw material used for risk rating and related mitigating controls. Risk rating takes the clients' various characteristics into consideration (country, type of client, activity/industry, 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').



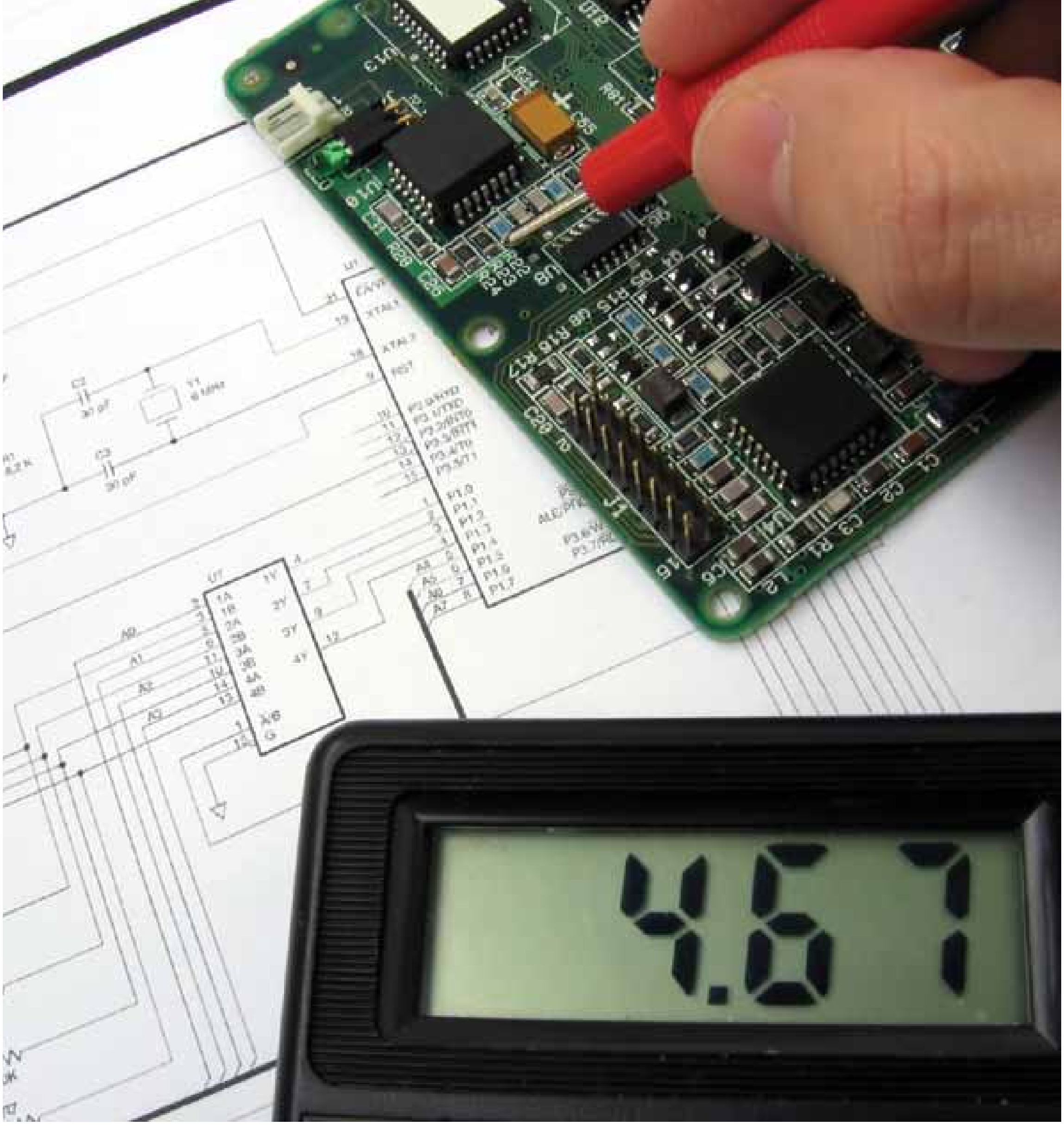
Furthermore, in order to generate useful and reliable queries and statistics, it is essential to ensure that static data is in a consistent and harmonised format. For instance, if nationality data for the United States is inputted as 'U.S.', 'USA', 'United States', 'America', 'California', etc., the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



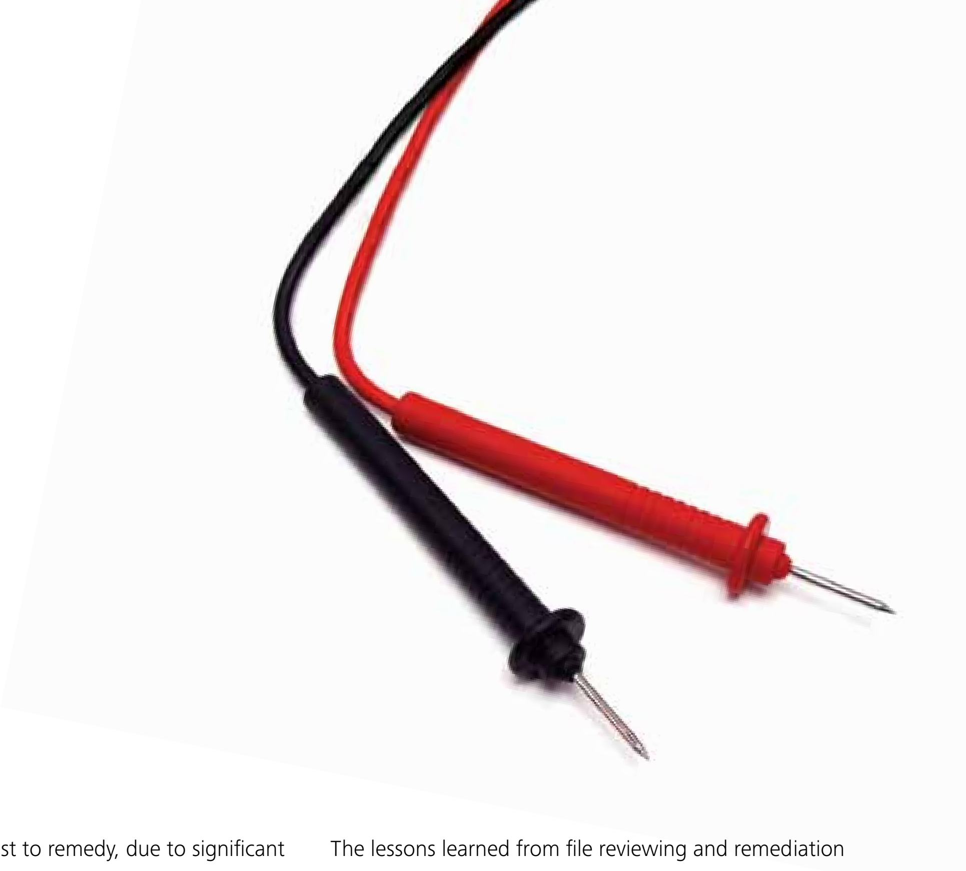
Client data is also used when reviewing the generated alerts to analyse the coherence with the initial account purpose and expected transactions. Here, information on the source of wealth required by article 24 of CSSF regulation no. 12-02 proves valuable, as it provides the professional with a context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