Challenges and trends in anti-money laundering and counter terrorist financing

"Business must harness the power of ethics which is assuming a new level of importance and power."
James Joseph[44]

There is a set of capabilities that can be considered under an AML/CTF map for financial institutions, which are intended to allow the identification, management, control, and oversight of ML/TF. This map includes (i) the framework and governance; (ii) the organizational structure; (iii) the business processes (including KYC, customer risk assessment, sanction screening, as well as transaction monitoring or payment screening, amongst others); (iv) the technological infrastructure; and (v) the data infrastructure and analytics capabilities (see figure 1).

Framework and Governance

At the foundation of their AML/CTF programs, financial institutions are enhancing their risk framework and governance models, to ensure both a comprehensive scope, as well as an effective embedding into the business. To this end, the framework includes the process of risk assessment, setting standards and policies, and ensuring robust risk management through a three Lines of Defense model.

Risk assessment

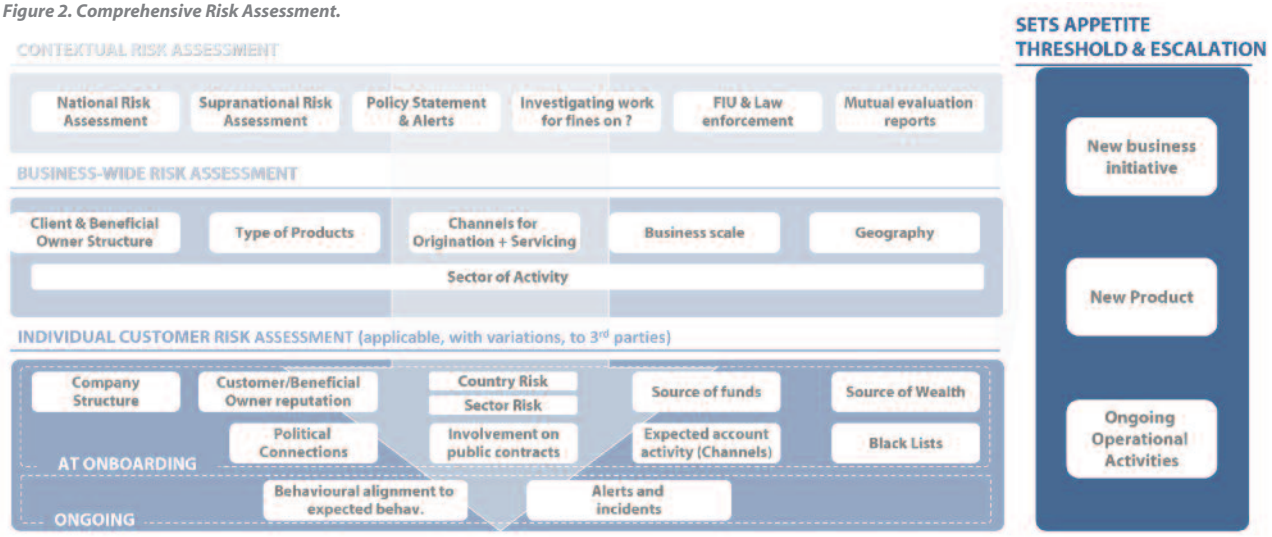
The Risk Assessment is a mechanism to understand the sources of risk, and it is one of the central components of the approach of a firm to AML/CTF.

The process of risk assessment has four main components that can be implemented: contextual, business-wide, customer and third-party risk assessment.

[44] James Joseph Sylvester (1814-1897) was an English mathematician who made important contributions to the field of matrices (he coined the terms matrix, invariant, discriminant and others), as well as to the theory of algebraic invariants (in collaboration with A. Cayley), determinants, number theory, partitions and combinatorics.

Figure 1. Generic map of AML/CTF capabilities in an advanced financial institution.

Figure 2. Comprehensive Risk Assessment.



Contextual Risk Assessment

The starting point of the Risk Assessment is a comprehensive review of the business model, as well as the context in which such business is conducted. There are many drivers for this analysis (see figure 2). In addition, an important input to this process is the regional / local Risk Assessment provided by the corresponding regulatory authority. In many countries, the supervisory authority has the mandate to perform a comprehensive Risk Assessment on AML/CTF[45,46,47].

Business-wide Risk Assessment

The business-wide Risk Assessment is the mechanism that enables financial institutions to assess, for each part of its business and within it[48]), where the major risks are.

Moreover, the business-wide Risk Assessment provides the framework and context in which to assess the AML/CTF risks in new product design as well as in individual business relationships, enabling a comprehensive review of the relationship through the different risk factors that impact the business.

Setting up a formal process, involving the right subject matter experts in the business, and ensuring that the risk assessment is reviewed on a continuous basis are some of the industry practices in advanced firms[49].

Customer Risk Assessment

At the most granular level, financial institutions perform individual Customer Risk Assessments (CRAs) to analyze the arising risks at the point of onboarding of a new client, as well as throughout the lifecycle of the client. This assessment shall include a minimum set of factors, which regulators have provided (e.g. sources of wealth and funds or specific country and sector risk factors)[50,51].

Historically, the data and mathematical capabilities devoted to CRA have been limited, triggering customer classifications that did not always discriminate high-risk clients, or that inadequately classified large number of customers into medium or high-risk buckets, with the corresponding operational effort required on monitoring, and the impact on customer experience.

As a result, financial institutions have devoted significant investment to get a more accurate risk-based approach and risk management. Currently, the efforts are focused on simplifying the taxonomy of models aligning to a common set of families of variables (e.g., Customer, Transaction, Channel, Product, Region), that are used consistently across the organization, to ensure completeness and adequate discrimination[52].

[45] See, for example, Article 6(5) of (EU) 2015/849 (The Fourth EU Anti-Money Laundering Directive), which requires the EBA to issue an Opinion on the risks of ML and TF affecting the EU's financial sector every two years.

[46] See the 'Opinion on the risks of money laundering and terrorist financing affecting the European Union's financial sector'.

[47] FATF (2013). https://www.fatf-gafi.org/documents/documents/nationalmoneylaunderingandterroristfinancingriskassessment.html

[48] It depends on its sector risk, business scale, customer and beneficial owner profiles and structure, the product types and complexity, channels used for distribution or servicing, transactions, and geographies.

[49] This process allows to formally include AML/CTF in the Risk Appetite framework, since it drives the operational activities in the business and strategic decisions in the new products approval committees, new business initiatives (like mergers, acquisitions, etc.) and new transformation projects.

[50] EBA (2017a) https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf/66ec16d9-0c02-428b-a294-ad1e3d659e70

[51] FCA (2022). https://www.handbook.fca.org.uk/handbook/FCG.pdf

[52] The more advanced financial institutions already use machine learning algorithms and behavioral models to assess the customer risk. These algorithms are trained and calibrated with historical data and, when required, with expert judgment, with significant improvements in accuracy versus traditional models which primarily consider expert judgment.

Third party Risk Assessment

Finally, some financial institutions rely on third parties to execute part of their day-to-day activities, from brokers and intermediaries to outsourcing operational activities, the provision of training, advisory, technological infrastructure services, etc. Depending on the nature of the business, these third parties can also expose the organization to AML/CTF[53] (or other forms of Financial Crime).

Therefore, it is common practice to have a fully integrated approach to third party vendor risk management to assess the underlying ML/TF risks. To this end, procurement teams undertake specific training to be able to act as a 'first line of defense' and perform the comprehensive assessment.

Standards and policies

A comprehensive body of documentation that specifies the standards to be followed across the organization is one of the strategic pillars of any AML/CTF framework, and one of the most effective mechanisms to mitigate the risk.

The most advanced organizations have the following elements in place:

- A policy architecture that, starting from a framework of documentation, progressively cascades down into business specific standards, as well as procedures and guidance instructions[54].
- Adequate mechanisms to effectively communicate and embed those policies into the actual BAU activity of the organization. These can include the existence of a web portal where the documentation is accessible to the relevant employees, together with a comprehensive training and awareness program and effective communication process to ensure that any relevant addition or change to the policy landscape is immediately communicated across the organization).
- Well-established operating model that enables policies to be reviewed and updated regularly, so that new regulation and emerging risks in the business, or lessons learned from AML/CTF incidents, are adequately and timely updated in the documents, and communicated across the organisation. Senior Management should drive this update, and the effective integration of the policies in the business processes[55].

The three lines of defense model

As with other risks, a robust three lines of defense (LOD) model is one of the pillars of the AML/CTF management framework, since it establishes the responsibilities for the identification, management, control and oversight of the underlying risks.

Financial institutions have reinforced their lines of defense model by performing a more granular split of responsibilities and accountabilities between them.

[53] EBA (2017b). https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf/66ec16d9-0c02-428b-a294-ad1e3d659e70

[54] Each document contains references to the risks it refers to (connected to the Risk Assessment when applicable), as well as to the external references (regulation and legislation, industry guidance etc.) that allows compliance and traceability.

[55] EBA (2017c). https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf/66ec16d9-0c02-428b-a294-ad1e3d659e70

First line of defense

The first line of defense is ultimately responsible for the identification, management and control of the risks originated in the conduct of business, as well as being in compliance against internal and external regulation. It maintains the relationship with the client, which involves carrying out basic KYC activities[56], and monitoring of the risk profile[57]. It is also responsible for deciding and coordinating customer exits.

In order to ensure the professionalization and standardization in the ways of working, and adequate resourcing, the more advanced institutions have formalized the role of an AML/CTF function or unit in the business that supports the business teams in the exercise of their accountabilities (see section on Organizational Structure).

Second line of defense

The second line of defense is in charge of setting up the AML/CTF framework, issuing policies (to adapt external regulation to the internal reality of the business) and eventually oversee their adequate implementation. In most financial institution, there tends to be also an element of advisory to the first line in complex cases of customer onboarding and exits, as well as in the case of new product / service development, etc.

In advanced financial institutions, the second LOD develop a formal oversight plan with different actions which combines the input obtained from different sources with the specialized knowledge about the business and firm-wide risk assessment or areas of regulatory concern. The action within the plan might include the issuance of new policy or guidance, more frequent management information of particular topics, increased sampling of cases, or more 'intrusive' thematic reviews and specialized on-site inspections.

The second LOD also produces regular management information and reporting to the internal governing bodies, to keep them informed of the evolution of the risk profile of the organization and any relevant point for escalation (e.g., gaps in the control environment, new high-risk relationships etc.).

The Head of AML/CTF oversight usually reports to an executive level: Chief Risk Officer, Chief Compliance Officer or Head of Legal / General Council, or in its case, a member of the Board of Directors[58] or within the Senior Management. Such nominated officer[59] is an individual with ultimate responsibility for the oversight of the framework and all the activity associated to AML/CTF. This individual and their team act as the central point of reference for both independent and effective challenge, as well as for advisory on specific, complex topics.

Third line of defense

The third LOD usually lies with the Internal Audit function of the organization. As with the rest of risks, this is an independent function from the business and the risk organization, reporting directly to the Board Audit Committee. Their responsibilities are to evaluate and assess the comprehensives and effectiveness of the framework defined by the second line of defense, its level of adoption by the first LOD and the level of independent oversight and effective challenge that the 2nd LOD performs.

The 3rd LOD has its own, independent audit plan that receives the 1st LOD and 2nd LOD management information as input and develops its own set of audits.

Organizational Structure

Specialized functions

In the last decade, financial institutions have been under intense pressure to reduce costs, given the sustained period of low interest rates to which they have been subjected, and the added financial impact of the pandemic. At the same time, they have been expected to improve the effectiveness and efficiency of their operations to increase the number of productive alerts and detection of ML attempts.

In terms of effectiveness, there is a trend to further professionalize certain functions within the AML/CTF function. Some examples include:

1. The creation of specialised teams of Quality Control / Quality Assurance in the first line of defence, which use a full set of techniques to perform advanced sampling in order to identify failures in the compliance against policies and procedures and raise recommendations for improvement.

2. The creation of specific Assurance and Oversight functions in the second line of defence. In line with the discussion

[56] For example, customer information gathering, identification and validation, CDD (or Enhanced Due Diligence, when required) and Customer Risk Assessment.

[57] This includes the ongoing monitoring of transactions (using in general advanced models to detect outlier behaviour and well-known money laundering strategies), screening of payments against watchlists, etc. As in the case of the onboarding, the analysis and clearance of low-level alerts tends to happen in the business as well, and escalation to the second line of defines happens only in those cases of suspected true positives.

[58] In certain jurisdictions it is required that the institution formally designate a member of the Board of Directors or within the Senior Management as the officer ultimately responsible for compliance with the regulation. See, for example, EBA Guidelines on the role of AML/CTF compliance officers, EBA/CP/2021/31. See also The Financial Conduct Authority ML 7.1 The money laundering reporting officer.

[59] Nominated officer is not necessarily considered a formal role. For example, in the UK regulation, it recognizes the role of a nominated officer', as does the role of a Money Laundering Reporting Officer (both roles can be put onto the same individual, see Financial Conduct Authority Handbook).

.

above, these teams act as a layer of execution of the oversight plan and performs deep dives in the form of detailed, specialised revision work on specific subject matters.

3. The creation of AML/CTF analytics teams. They tend to incorporate other sub-risks in addition to AML/CTF. (e.g., fraud) and are usually very business-oriented teams, identifying any new trend in the market.

4. The creation of specialised capabilities around change and remediation in the business. The combined effect of the multiple layers of control and oversight translate into a portfolio of recommendations, issued from the Quality Control teams, Internal Audit teams and Supervisory reviews.

Centralization and the creation of centers of excellence

In connection with the drive for more efficient operations, a number of large financial institutions have pulled the lever of centralisation of some of the operational activities within their AML/CTF teams, creating centres of excellence. Some of the operational activities that have been centralised include the Customer Due Diligence, which incorporate the checks and controls around KYC, and the performance of the Customer Risk Assessment, etc[60]. These teams usually have a specialization by Retail and Corporate, to account for the differences in the KYC / KYB processes. Some Institutions have a specialized team in KYS (Know your Supplier), and perform the AML/CTF as well as the Fraud and ABC assessment of their Suppliers in a single team.

For large International Financial Groups, a natural evolution in their centralization journey has been the regionalization of activities (i.e., the creation of centers of excellence at a regional level) with the corresponding benefits in terms of better management of the pool of resources, removal of duplication, streamlined organizational structure and better career paths and cross training opportunities for the workforce.

Although outsourcing some of the operational activities is an option, there are a number of factors pushing some financial institutions to on-board back the outsourced capabilities and develop the skillsets within the organization. Some of the factors are the increasing regulatory demand around outsourced activities that are critical to the organization, the associated need to build strong oversight and control structures around the outsourced services, the level of operational excellence expected by the different stakeholders, or the reputational impact of operational failures.

[60]There are further examples such: the execution of name screening and associated maintenance of watchlists; the performance of Transaction Monitoring (as in the case of CDD, with a natural split between Retail and Corporate); the execution of Payment Screening; the operational procedures associated to customer exits; the production of standardised Management Information and Reporting and some of the activities specified above, including Quality Assurance, Change and Remediation or Data Analytics.

Integrated approach to financial crime risk

Some of the most complex recent Financial Crime incidents involve a combination of stealing of credentials and impersonation, illicit use of privileged access to commit a Fraud, and multiple mechanism to launder the profits.

In that sense, a common trend in some of the most advanced financial institutions, according to regulatory advice[1], consists of achieving a convergence towards a unified Governance model that incorporates all sub-risk types (ML, TF, tax evasion, fraud and Cybercrime) into a single framework.

The natural synergies that arise by addressing the different sub-risk types of Financial Crime under a unified model and the consequent opportunity for efficiency explain the adoption of this model:

- There is a strong analysis of a new customer at the point of origination of the relationship, with a significant amount of common information cutting across customer identification, validation, name screening, customer risk assessments, etc.
- There is a component of ongoing monitoring, also with overlapping datasets around transactional and payment information, which can be merged into a single data repository for the purpose of exploitation.
- Finally, there is an investigation process that requires workflow tooling capabilities, strong record keeping, documentation and reporting.

In large financial institutions there is some level of integration. However, there is still room for improvement in terms of achieving full integration. Some of the best practices in the industry include:

- A single framework for risk identification, management and control, including a common risk taxonomy across all risk types, a common Risk and Control self-assessment, etc.
- Common underlying data infrastructure, aiming for a single, "360-view" of the customer and its data-self, together with its transactionality.
- Common framework and technological infrastructure for alert implementation and detection, as well as for alert management.
- Centralised organisations, which incentivise information sharing and a holistic approach to risk ownership and management, without gaps that financial criminals can exploit.
- Operational centres of excellence capable of providing operational capabilities across the different risk types, with cross-trained individuals capable of managing those cases.

Given the significant number of operational people currently in charge of the identification and management of the different financial crime teams, and the natural silo-ed approach with which they were originally setup, the opportunities of this journey towards integration in terms of removal of duplication, increased efficiency and effectiveness is quite significant.

[1]See, e.g. See FCA's A firm's guide to countering financial crime risks, https://www.handbook.fca.org.uk/handbook/FCG.pdf

Workforce planning and skillsets

The most advanced financial institutions have been able to connect their target ambition around AML/CTF, as reflected in their Risk Appetite and strategy, with their workforce's needs. In those cases, there is a thorough analysis that:

i. Starts with the business-wide Risk Assessment, expected business growth and changes in the risk profile and strategic initiatives that are expected to change the ways of working.

ii. Make an informed projection of the required capacity to tackle the AML/CTF strategy[61]. Some of the best practices in the industry involve the building of dimensioning models for the operational teams to be able to connect, at an operational level, demand of capacity with supply.

iii. Develops a strategy to ensure that such capacity will be in place is then designed and implemented. This includes training or recycling existing staff and hiring new talent.

In the last few years, workforce planning exercises in some of the more advanced organizations have identified the need to reinforce the teams with:

1. Quantitative and analytical profiles capable of understanding the business and the underlying risks, and building mathematical models using machine learning techniques.

2. Knowledge on specialised new payment technologies, including crypto currencies.

3. Multi-skilled individuals able of capitalize previous experience on different sub-risk types within Financial Crime, which become AML/CTF subject matter experts.

Business Processes

Financial institutions have devoted significant time and effort to streamline the business processes associated to AML/CTF. The pressure to reduce cost and improve efficiency has opened the door to advance automation technologies, business process management platforms and advanced modelling. Moreover, those improvements also have a positive impact on customer experience, 'asking things once', etc. Processes such as KYC have been significantly simplified and strengthened.

KYC: Risk Assessment, Customer Due Diligence and Enhanced Due Diligence

Delivery channels have pivoted from a branch-centered model to a self-service, non-face-to-face one, fostered by enabling technologies, institutions pursue of cost reductions, and the Covid-19 pandemic. Digital Customer Risk Management shifts from being a penalizing channel factor to become the usual means of management, which requires a stricter control over bank-customer communication. Unfortunately, it is harder for financial institutions to verify who they are doing business with and the real purposes of the business relationships. Disruptive new technologies and modern procedures allow financial institutions to mitigate their AML/CTF exposure through improved Due Diligence mechanisms. Nonetheless, some of these improvements have also become strenuous for the customer because of constant requests for documentation, often via paper with no digital alternative.

Automated self-servicing solutions[62] through digital channels, actionable by the user, using a Digital ID and Biometric data empowers customers during the onboarding process, periodic reviews and recertification. Moreover, it eases automated record keeping of customer support during due diligence process, which can be determinant in a potential investigation process. Likewise, Digital ID and Biometric data will counteract identity fraud.

These self-servicing solutions recognize the distribution of customers by segments, defined and calculated by Compliance departments backed by AI techniques. As a result, customer segmentation can improve KYC information capture aided by dynamic onboarding questionnaires. Consequently, it is key to refine the customer journey development-lifecycle, to ensure quick time to market of new enhancements in the KYC process and adapt lithely to new regulations.

KYC policies and procedures should be periodically reviewed to mitigate risk and increase financial inclusion. In this respect, some citizens are not able to open bank accounts or access to public aid because of the difficulty of gathering the required identification. Hence, financial institutions should avoid rigid, box ticking CDD measures and bet for behavioral and contextual assessments.

Ongoing Monitoring (Transaction Monitoring, Sanction Screening, Payment Screening,)

Transaction Monitoring is a heavy lifting process[63]. Aggregating all transactions, accounts, and customers in order to calculate the likelihood of each scenario requires high amounts of compute and memory capacity. Cost-benefit analysis is a contentious topic amongst Regulatory Compliance Department. Legacy systems might be enhanced to cope with performance demands, but there is a soaring necessity for cutting-edge technologies with higher provisioned capacity as more data is integrated in the models.

[61] This capacity is articulated in terms of number of people, skillsets and expertise, locations, etc.
[62] See EBA Guidance on the use of remote customer onboarding solutions. https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-countering-financing-terrorism/guidelines-use-remote-customer-onboarding-solutions.
[63] European Banking Authority. (2021).

Elements of human resources management

Culture and behaviors

Corporate Culture refers to the beliefs and ideas that a company has and the way in which they affect how it does business and how its employees behave [Cambridge Dictionary]

Culture, ways of working and staff behaviors have been identified in several thematic reviews and enforcement actions triggered by supervisors, regulators, and national agencies as one of the root causes of gaps in the AML/CTF framework.

For this reason, financial institutions that have advanced AML/CTF programs tend to incorporate an ambitious culture, aimed at embedding the right behaviors in the conduct of business. Some of the components of the cultural framework of the organization include capabilities around the following elements:

Staff recruitment and vetting

Before their onboarding, the individuals that will bear any responsibility associated to AML/CTF (both internal workforce or a third party) should go through a process of vetting, to validate to the extent possible that they have the right work ethic and integrity, and that nothing in their background would expose them as targets of organized crime[1].

Training and certification

Training and awareness programs involve generic courses for all the bank's employees, specific training for the AML/CTF function and training for members of the Executive Committee and Board, covering all the range of crimes and criminal strategies that are pertinent to the organization[2].

Engagement from the management

Senior management play a key role in terms of culture embedding. In advanced financial institutions, individuals that are close to the operational levels of risk framework execution feel safe escalating issues and concerns associated to business activity, and these escalations are treated anonymously and diligently. Whistleblowing mechanisms are in place and are regularly used by employees to raise concerns, or debates in decision making forums.

At a Board level, in advanced financial institutions, the Board members have both the knowledge and the management information to understand the AML/CTF risks and perform effective challenge to the executive roles.

Incentives and performance measurement

The incentive and remuneration mechanisms should be aligned to the desirable behaviors of the workforce, and to an adequate delivery of individual accountabilities as per the firm's governance model. Additionally, the incentive scheme shall not encourage unacceptable risk taking that is above the appetite of the organization.

The most advanced financial institutions have an objective setting mechanism that incorporates key risk and performance indicators associated to AML/CTF that are quantifiable, as well as qualitative indicators that reflect the desired behaviors.

Communications

As one of the mechanisms to propagate culture and to increase awareness across staff, some financial institutions build strong communication programs around their AML/CTF framework. These are run as professional communication campaigns, with a clear segmentation of the audience, selection of content to be targeted to each audience segment, delivery channel, etc.

[1]The more advanced institutions have a bespoke vetting process for the different roles within the organization, including different levels of seniority and responsibility, as well as different risks that they will be more exposed to depending on their role (e.g. customer facing clients, financial investigation unit, second line of defense specialist, etc.).

[2]The training programs might include a process for continuous review and enhancement. Moreover, there is specific responsibilities to formally review the training materials to incorporate new evolutions of the internal policy and regulatory landscape, emerging risks, new regulatory publications, etc. There are also programs for industry certifications, which can be connected to career paths and career development incentives.

A configuration to increase performance without infrastructure investment is the execution of scenarios based on customer segmentation, instead of running all scenarios for all the data available. This is harmonized with a Risk Based Assessment, because scenarios are customized to adapt to the Institution's risk profile and business reality (customers, geography, product catalogue, etc.). Another option to increase efficiency without additional resource allocation is performance simulation (number of alerts, False Positives, False Negatives, etc.) in a sandbox environment before deploying the scenario into Production. A third option is to run the scenarios only against susceptible customers, omitting, for instance, government and public agencies with very low risk. On a related note, potential links with sanctioned entities could be identified through retroactive batch screening over the complete customer portfolio, considering those customers as high-risk individuals to be investigated.

The business processes around sanctions have suffered a significant transformation in the last months, as a result of the Russia invasion of Ukraine, and the associated legislative actions that the European Union, the US, the UK[64] and other geographies took. Financial institutions have invested resources in both interpreting the restrictions and in operational improvements in terms of list management. In some cases, this has meant an acceleration of programs aimed at implementing a Centralized List Management Platform that aggregates files from different treasury departments and vendors, cleanses the data and then disseminates them amongst all group entities according to their local regulations and the group's policy eliminates duplicities and increases oversight of the Sanctions program[65].

Transactional scanning[66] and customer name scanning during onboarding shall run in real time. Therefore, strict Service-Level Agreements (SLAs) are required for list upload, as most systems cannot scan during a list refresh. On the other hand, when black or grey lists are updated, a batch scanning is required on all customer records against changes in the lists. This process should not interfere with the online processes and should run on a separate queue, as lists changes are very frequent, even several times a week and time consuming, given the high number of customer records.

Alert Management and Investigation

The implementation of a specialized vendor solution per module, and at times more than one tool per module from different vendors, isolates alerts as Case Management systems are not integrated. What is more, Compliance Officers do not have access to all the data and their procedures may vary due to their tool. To gain a holistic view of the customer risk and standardize alert investigation and reporting, it is indispensable to consolidate KYC, Screening, Transaction Monitoring, and Alert & Case Management data into a single platform. Consolidating basic information required for an investigation before the alert is assigned enhances the time per alert plus automatic notifications to Compliance Management when an alert is pending authorization.

Machine learning models are helpful to score alerts, in order to discriminate potential false positives. Then, AML/CTF Function should have established a clearly defined and objective workflow for the review of alerts, with a prioritization criterion to analyze them[67].

Engagement with Law enforcement and SAR

Even if risk detection is successfully implemented, bad reporting could tamper the process. Financial institutions must comply with their FIU's expected SLAs, adapting their reports to a specific format that is subject to changes. Some regulatory steps that do not require manual intervention, for instance Currency Transaction Reports (CTRs), applicable in USA, leave room for automation. At the same time, proactive detection of CTR Exemptions is a quick-win enhancement of the CTR function. Nonetheless, AML Management should periodically review the decision-making process of exceptions to gain control and understanding.

Communication with the lines of business, who have a direct contact with the customers, demands dynamic channels to

[64] See the Economic Crime (Transparency and Enforcement) 2022 Act (the ECTE Act) in the UK, OFAC Frequently Asked Questions 1007 and 1010, or the up to eight packages of sanctions imposed by the EU on Russian individuals and companies.

[65] Sanctions platforms need customization rules to avoid scanning irrelevant values (PO Box, #, double spaces…).

[66] In addition to the analysis of money transfer, the digital footprint is a rising method for red flags. The IP Addresses collected during customer's operations, associated with transactions and logins, shall be routinely monitored and compared with the ones ingested during onboarding to detect misuse of an account from a High-risk/Sanctioned country or account theft. The detection of Tor associated IP addresses is fundamental, as it might reveal connections between the customer and criminals from the darknet.

[67] For example, based on risk profiles, transaction amount or matching scores). This process is only possible if carried by specialized AML teams to handle the sleuth of complex organizations and manage whitelists.

resolve questions and transfer documentation within the regulator's timeframe, and applying penalizations on client managers in case of frequently repeated mistakes when collecting customer information. Finally, repeated warnings and foundations of rejected reports require detection and data profiling to understand the root-cause and palliation. Data Quality between ATMs and Bank databases with previously recorded customer information is worthy, but also to identify reporting mistakes and duplicities before filing them to the regulator.

Management Information and Data

Management Information

The Management Information on AML/CTF enables measurement, visualization, communication and effective management of the underlying risks. In that sense, the best practice in the industry includes the adoption of industry standards around data governance and management and reporting practices (e.g., BCBS 239[68]).

The management information produced should detail the changes in the Risk Assessment at a firm-wide level, as well as a representation of the risks associated to new business relationships (including new business relationships per risk category, any new high-risk relationship, etc.). For existing relationships, the top management of the organization should receive timely information on the outcomes of the ongoing monitoring activities (e.g., transaction monitoring, payment screening, periodic customer reviews), as well as the summary of the Suspicious Activity Reporting and statistics on positive hits above and below a specific threshold. The reporting structure should also contain the exit of existing relationships, and its rationale.

In particular, the more advanced financial institutions incorporate, in the reporting to the Board, Board delegated Committees and Executive Committees, a comprehensive set of metrics and qualitative information to ensure that all the underlying risks associated to the business are taken into consideration. Additionally, for more operational teams, institutions have developed dashboards containing real time KPI and KRI metrics, with the option of extracting insights on the data in more detail to facilitate the identification of weaknesses in the process and draft long-term strategies.

Other good industry practices include the incorporation, in the regular management information escalated to senior management, of the open issues at portfolio level stated by Quality Assurance, Internal Audit or Supervisory investigative action[69]. This view also overlays, on top of the remedial action, the information on strategic transformation of the AML/CTF operations and provides in this way a single view of change across the discipline.

[68] Basel Committee (2013a). https://www.bis.org/publ/bcbs239.pdf

[69] In the more advanced organizations, the reports to senior management include a section on Regulatory Liaison or Industry engagement. This usually contains an element of horizon scanning for new regulation or legal requirements (and the anticipated downstream impact in the organization).

Data Management and Data Quality

Data has been one of the key areas of evolution and investment by financial institutions in the last years. There is recognition that insufficient or poor-quality data[70] is one of the most relevant factors that impact the ability of a Financial Institution to identify, manage and control ML/TF risks. In addition to classical, manually driven data quality remediation, firms are making extensive use of advanced techniques for data discovery as well as analytical methods like fuzzy logic or natural language processing to perform data matching and harmonization.

There are several Data Management capabilities supporting the AML/CTF functions that are instrumental. One of them is a Data Quality capability to proactively specify business rules and data quality standards around the critical data elements used in risk identification and management. Also, a Data Catalog that allows harmonization of data across different repositories and engines and allow data stewards to better understand the business meaning of the data, classify the data collected and consumed in each process, and alert appropriate stakeholders in case of a data issue. Moreover, financial institutions are investing heavily in data lineage capabilities to enable end-to-end traceability of the data from the point of use back to the point of origination.

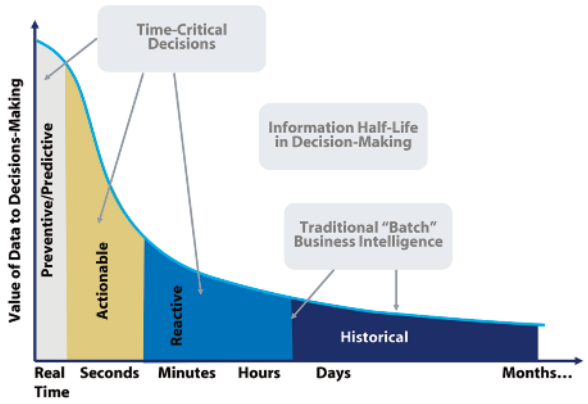
Even the most advanced AML/CTF systems' automatic detection are not trustworthy if the data is wrong. Quality rules implemented on the transactional, front office systems will ensure the correct data generation and consistency rules will confirm the right data feeds into the AML/CTF systems.

Data infrastructure and demands on an AML/CTF Data Model

The need for Management Information implies a demanding data infrastructure[71]. It is desirable to capture, store, process and manage sensitive information with the highest standards. The technological modules used for AML/CTF can excel at their analytical capabilities, but duplicated data flows to different, siloed technological component is highly inefficient from the transmission standpoint.

For this reason, it is important to have a unique data repository accessed by all technological components and business processes involved in the AML/CTF framework. This way, each process (e.g., Customer Risk Rating, Alerts, Case Results, Suspicious Activity Report, etc.) uses data from the central repository and store their results back in the same repository, making them instantly available for other processes and parties involved. Financial institutions that operate in multiple countries can centralize their tools and repositories for whole regions or even globally. These solutions will improve compliance oversight, and reduce costs in duplicated vendor licenses, infrastructure or departments in the group entities. Therefore, leveraging these external sources to complement the available internal information is a trend in most financial institutions.

Figure 3. Time reduction of value of data for decision making.



Source: Perishable insights, Mike Gualtieri, Forrester

However, financial institutions can no longer obtain by themselves all the necessary information to properly identify and assess potential risks inherent to their activity. In a digital-centered industry, accumulated data can be sold or shared with other parties. Hence, external sources such as reputed bureaus, national crime agencies, court judgments and public registries are recommended sources for model enrichment.

Disruptive technologies, modern customers' behavior and natural disasters require financial institutions to redesign their transaction monitoring strategies. Models undertrained on new AML/CTF techniques do not provide the ability to respond rapidly to Financial Crime risk. Consequently, certain scenarios should automatically execute when particular external events occur (new products, lockdowns, catastrophes, conflicts etc.).

Historical analysis is a key practice in these cases. Even if the financial institution misses any scenarios during a crisis, red flags can still be found against these temporary scenarios and Suspicious Activity Report submitted. Behavioral Monitoring is one of the current trends in the industry, supported by the newest machine learning techniques. Behavioral Monitoring first defines how the products and services are expected to be used. Secondly, it looks at historical behavior, expected behavior, peer-group behavior and identifies behavior changes, consuming all available data to detect Financial Crime risk.

In the Case Management area, the widespread use of social media is again requiring for the ingestion of unstructured data and the use of graphs to find potential connections between customers and criminals. Finally, standardized reporting templates using data pooling tools, which combine datasets from multiple sources, and automated generation of SARs will accommodate any format changes required by the FIUs, reducing rejections.

[70] Basel Committee on Banking Supervision. (2013b).
[71] Basel Committee on Banking Supervision. (2013c).

Technological infrastructure

AML/CTF tools can no longer rely only on a relational DataMart as a central database, as it is now receiving unstructured data where NoSQL and Data Lakes become more effective. It is of utmost importance to implement real time detection technologies to prevent risks associated with unnoticed errors and improve customer experience (see figure 3). Financial institutions still rely on queuing and file management systems to send transactions and notifications between applications. Transactional and name screening (or cases outside AML/CTF, like Fraud audio detection) benefit from real time analysis. For the latter, machine learning libraries for Natural Language Processing (NLP) are appropriate to collect, analyze and store audio information and, create alerts to the lines of business interacting with the customer, finalizing the call immediately to avoid sharing any personal information (figure 3).

Real time and unstructured data improvements result on spikes in transmission, processing, and storage activity, with major investments in new storage options and data migration. For this reason, migrating to a Cloud infrastructure is a sound solution to access new features for data management.

Regarding IP address screening, financial institutions need to coordinate amongst them and regulators to systematize the generation of lists containing non-trusted IP addresses, IP addresses from sanctioned jurisdictions or IP addresses flagged as suspicious. Alongside, analytical tools are available in the market to detect if customers are using a Virtual Private Network (VPN) to distort their real location. Application-programming interfaces (APIs) play a significant role in this new monitoring, as their logs should capture IP data that can be analyzed in real time, employing tools such as AWS OpenSearch or Splunk.

Robotic Process Automation (RPA) is one of the main technological trends that increases customer experience through automated self-servicing solutions. Virtual agents, chat-bots and call-bots can assist customers with structured and repetitive inquiries day and night without interruption, getting them in contact with a human resource for queries that are more complex. RPA is also a crucial improvement for Alert and Case Management, as these algorithms can ingest more data from more sources quicker than a human investigator, enabling faster analysis of a broader evidence base and, ultimately, more accurate resolution[72].

[72]For example, collecting and aggregating necessary data for an investigation, saves time to the AML Officer searching for documentation. Other repetitive tasks are subject for automation, for instance, flagging duplicated alerts of a single customer. More sophisticated systems will automate steps or results based on previous investigations and outcomes.

Some examples of data requirements and practices

Some jurisdictions such as the EU (e.g.: eIDAS) require financial institutions to capture and manage eIDs from any Member State for AML/CTF purposes, which is expected to reduce costs and human errors with better customer experience. This is significant for trust services, which are deemed to have higher risks due to their structure, short lifecycles and varied purposes.

In this respect, during any business relationship, financial institutions collect geolocation and IP Address information to later detect activity from undesirable locations or account theft. A robust Data Integration capability correctly connects the different fields with the questions shown in the dynamic questionnaires, thus segmenting the customer. FinCen[1] even recommends collecting the IMEI (International Mobile Equipment Identity) a unique 15-digit identification number assigned to each mobile phone, and device model of the customer's cellphone for convertible virtual currency operations. Financial institutions store their digital interactions with customers deploying semi-structured and unstructured databases.

As mentioned, financial institutions have to integrate information from external sources to enrich their models. Some of this information is easy to ingest, such as ultimate beneficial owner flags in public registries or records from a PEP list. Conversely, Adverse Media files can include audio or video format, which again highlights demand for unstructured information. Additionally, some jurisdictions require automated mechanisms to report any misalignments between public registries and data collected by obliged entities.

In terms of screening lists, there are also some industry good practices worth highlighting. Blacklists must not be modified, except for enrichment and aggregation, whilst white and grey lists shall be quick and easily updated by compliance departments to improve performance and comply with internal policies. This perspective has to be reflected when building a centralized list management system jointly with automatic notifications when lists are received, aggregated and disseminated. Statistics about record counts should be available and the system should expect automatic notification from the screening systems, reporting same list record counts loaded on their databases.

Other than that, in 2018, OFAC included the first virtual currency addresses in the SDN (Specially Designated Nationals and Blocked persons) list. These are digital wallets tied to sanctioned individuals and companies with whom businesses is prohibited, which structure is as described. These are digital wallets tied to sanctioned individuals and companies with whom business is prohibited.

One of the most relevant industry trends is the adoption of ISO20022 on SWIFT payments, which improves screening and monitoring performance by including XML tags. By contrast with current free-form messages, SWIFT payments will clearly specify the meaning of the fields, reducing false positives. Financial institutions are required to upgrade their screening and monitoring systems to parse these new tags and store them in appropriate tables and columns in their databases.

Reference of new SWIFT transaction information XML tags.

Digital Currency Address	XBT	158treVZBGMBThoaympxccPdZPtqUfYfT9
SDN list column	Currency	Wallet ID

[1]The Financial Crimes Enforcement Network of US seeks to safeguard the financial system from illicit use, combat ML and its related crimes including terrorism, and promote national security.