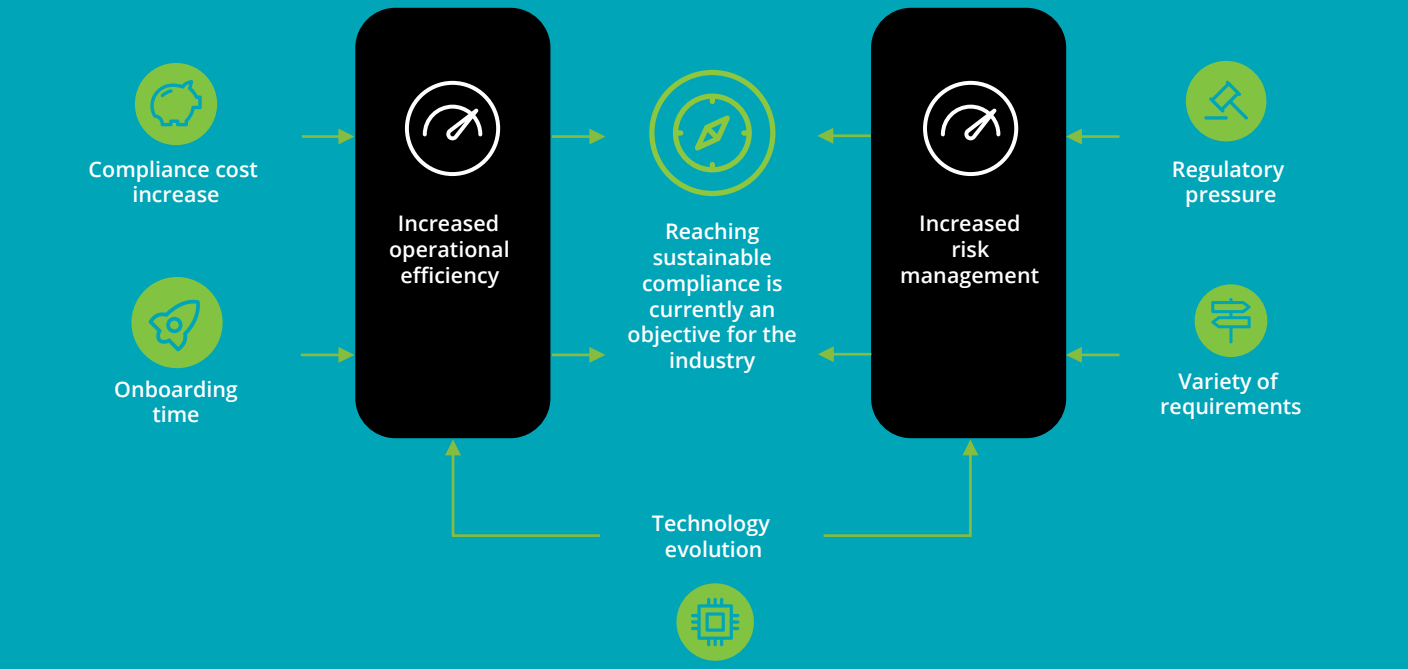
How should we tackle the new KYC challenges?

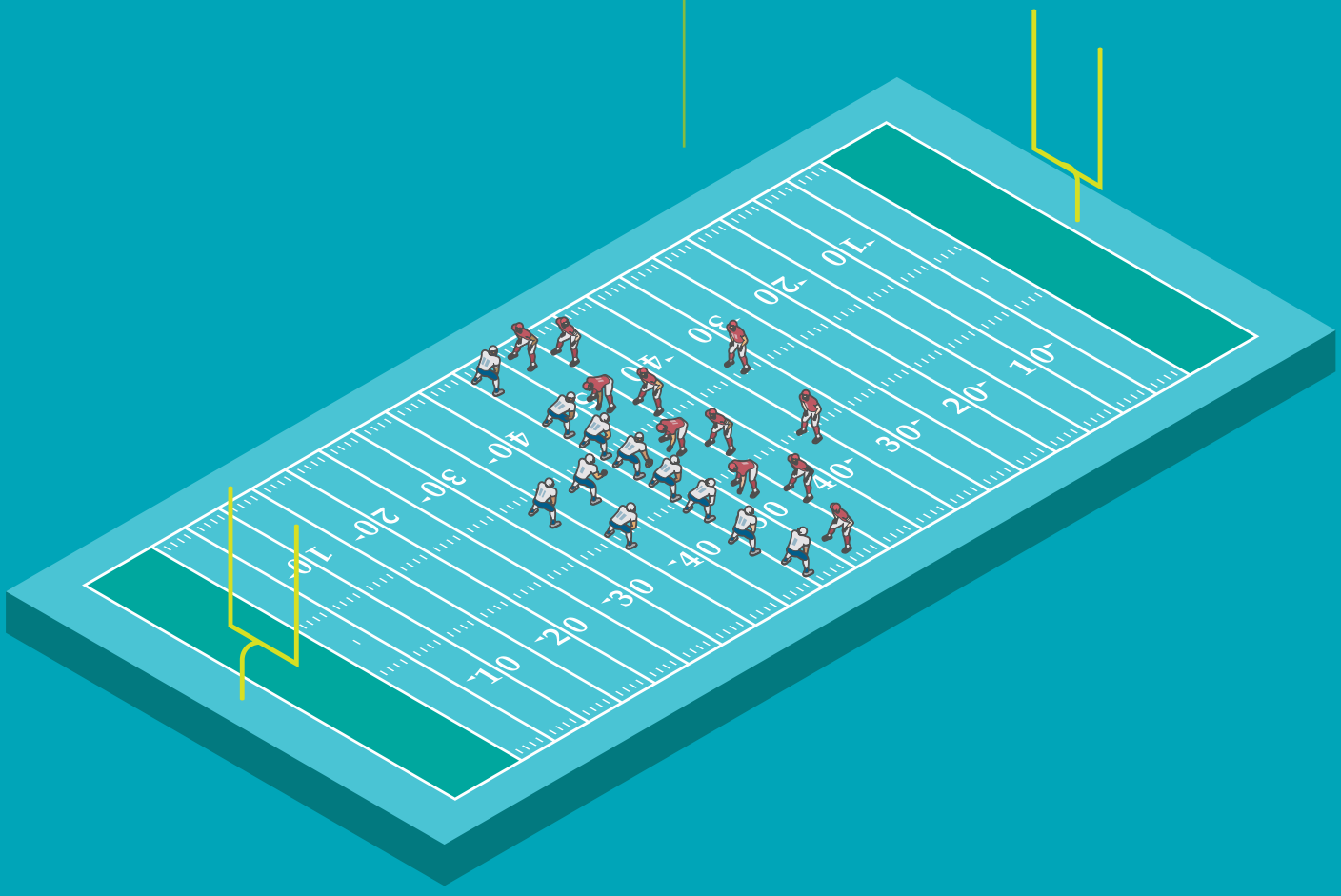
Maxime Heckel
Director
Operations Excellence
& Human Capital
Deloitte

Bastien Collette
Senior Manager
Operations Excellence
& Human Capital
Deloitte

In the aftermath of the financial crisis and several recent cases of fraud, money laundering, and tax evasion, today's worldwide attention is mostly focused on financial institutions' anti money laundering/ counter terrorism financing (hereafter AML/CTF) duties and obligations. The focus is especially on the way the institutions apply underlying controls on their counterparties. Legal frameworks and related professional standards have changed and are still evolving drastically, increasing compliance requirements toward market actors[1], which therefore increases pressure on regulators to enforce the rules.

1 FATF recommendations, 4th European AML Directive, national AML/CTF legislations, tax transparency regulations like FATCA or AEOI/CRS, etc.


Compliance cost increase
Onboarding time
Increased operational efficiency
Reaching sustainable compliance is currently an objective for the industry
Increased risk management
Regulatory pressure
Variety of requirements
Technology evolution



As a result, financial institutions are struggling to comply with this ever-evolving AML/CTF and tax transparency framework. The entire Know Your Customer (hereafter KYC) process chain needs to be enhanced to ensure that all counterparties' information is collected, qualified, stored, monitored, and screened, including related parties and the shareholding structure. The resulting risk assessment must be reviewed on a recurrent basis, including the risk of reputation, which until recently was often underestimated. On that basis, reaching sustainable compliance in a cost-effective way is an objective for the industry, now more than ever. This must coincide with an increased volume of KYC documents/data to be collected and processed, with strong requirements to decrease onboarding time, especially in the fund industry or in digital banking structures.

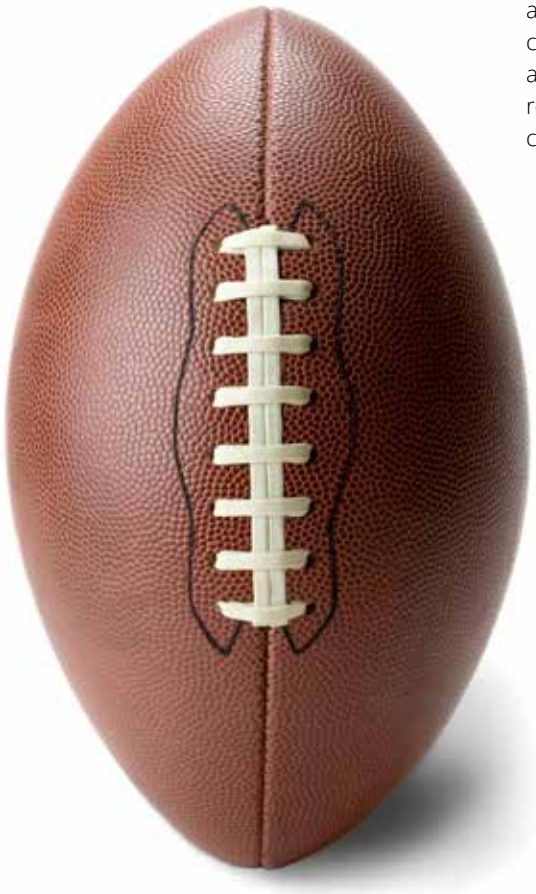
The new KYC challenges

Up until this point, it is clear that current AML/CTF practices are redundant within financial institutions and therefore inefficient, requiring every counterparty to exchange information with every financial institution in their operating network. The market is becoming increasingly ready to cope with next curve, which is why we observe rapidly emerging KYC utilities on the market.

Knowing that toggling between KYC utilities is neither efficient nor cost effective, we anticipate those utilities to be expanded over time to not only propose a KYC document repository but value-added services on top.

The utilities are central repositories that offer to collect, qualify, and store KYC documents and related signaletic data of institutions' counterparties. As a consequence, a synergy effect is created at both the information contribution and consumption sides, since mutualization of documents, data, and some KYC steps occur. Obviously, this is only happening if such a platform is able to show a high market adoption rate (i.e., critical mass of up-to-date documents/data).

This mutualization approach makes sense in a market where actors are progressively looking to reduce in-house involvement in non-core activities by outsourcing them to external providers. Nevertheless, a few blurry points remain. What is the point in having multiple utilities to cover the same feature? Can financial institutions satisfy their needs by subscribing to one utility only? Are those utilities able to cover local specificities, requirements, and several market segments? Those three questions symbolize the main issues with KYC utilities: they are only able to cover a limited scope of the KYC burden felt in the market, mainly because they address one or two main functions each (e.g., KYC documentary platform only, counterparty screening and risk scoring only, etc.) or cover a limited market segment (e.g., correspondent banking only, fund industry only, etc.). It is unlikely that a single player will capture the whole market and the entire set of business/technical requirements in AML/CTF. In the near future, multiple players will have to co-exist and specialize among specific areas (e.g., geography, line of business, etc.) and in the best case, provide "interoperability" among themselves. Knowing that toggling between KYC utilities is not efficient or cost effective, we anticipate those utilities to be expanded over time to not only propose a KYC document repository but value-added services on top.



Value-added services may include new generation onboarding and ongoing monitoring chains such as screening/adverse media search/background check, risk scoring, AML/CTF country risk assessment, on-site due diligence (when required), or FATCA/CRS accounts pre-classification and reporting.

Such end-to-end KYC managed services must also cover several jurisdictions, types of counterparties (financial institution, legal entity and arrangement, retail, etc.) and market segments (banking, fund industry, life insurance, corporates, etc.), allowing market actors to reduce their unit costs (savings through mutualization of technology, resources, and expertise), as well as the organizational/operational impact of seasonal peaks of activities (for instance QI/FATCA/CRS reporting).
It must be understood that even if an outsourced approach toward AML/CTF activities will help to reduce related costs while increasing risk management, it will not withdraw the ultimate AML responsibility from financial institutions. The compliance function is thus not coming to an end, and would instead be more focused on the risk-based approach maintenance, operations oversight, and diligence on the most risky cases, switching from an administrative (applying a "tick the box" process) to a real risk-based approach function.

Technology and data sources evolution

From a purely technological standpoint, we observe that most financial institutions are still using "generation 1.0" solutions, e.g., out of the box name screening (fuzzy matching), rules-based customer profiling, etc., whereas "generation 2.0" tools are offering new ways to perform counterparty due diligence (adverse media search rather than watchlist screening) or customer profiling (machine learning rather than rule-based engines). Such technologies are quite costly, mainly for small/mid-size businesses and especially knowing that Return on Investment (ROI) cannot be part of the equation.

This is also valid for market data sources where alternatives could be found to the usual and expensive consolidated "watchlists". Indeed, more and more counterparty screening solutions are relying on open source data and offer to identify corporate shareholding structures and related/linked parties as well.

This is certainly not an exact science (false positives will still be generated), nor fully ready yet, but underlying cost-effectiveness is promising. At the same time, it is important to keep an eye on other emerging innovative technologies such as blockchain, digital passport, or video/online client onboarding. These could play a significant role in automating the future of finance, assuming market actors can overcome the challenges related to these processes.

What's in it for a CIO

In order to keep the pace in this changing environment, CIOs should be focused on a few key priorities:

- Be conscious of upcoming KYC regulations, assessing the impact related to the additional information to be collected and stored in systems, data privacy, and new needs for business features that will be triggered.

- Review both AML/CTF and AEoI (Automatic Exchange of Information) application value chains to identify weaknesses and opportunities to create synergies; especially knowing recent multiplication of both data sources and regulatory needs (including recurrent electronic reporting).
- Monitor the evolution of KYC utilities, especially the interoperability dimension.
- Assess the cost-effictiveness benefit for replacing existing AML/CTF technology framework in favor of the most recent ones, for instance, drastically reducing the number of false positives (from counterparty screening or transaction filtering/monitoring).
- Assess the business case to mutualize related operations through externalization (i.e., managed services approach), and therefore accessing new technologies, enhanced KYC data, documentation framework, and dedicated expertise.

Conclusion

Answers to the above KYC challenges have to go through both increased risk management and operational efficiency. This implies that one must think and act differently:

- Financial institutions need to be more efficient while not making any compromise on service quality or compliance with regulations.
- Mandatory and high risk activities such as AML/CTF and KYC do not represent a differentiator across the competition.
- It is still possible to tweak the KYC chain, but not in a sufficient scale, since "gen 1" technology still used today shows a limited internal optimization potential.
- Duplication of AML/CTF tasks and redundancy of related controls within the financial institutions create significant inefficiencies at the industry level.

The entire model needs to be upgraded, and we think that externalization (and therefore mutualization of fixed costs) is the only way to generate substantial savings while increasing compliance level.

With regards to practical implementation, financial institutions should also ensure that service providers are ready to integrate near future technological evolutions. For instance, the use of blockchain technology enables cost savings and removes effort duplication across entities carrying out AML/CTF activities. Validated results would be recorded into the Blockchain in order to share encrypted and up-to-date KYC data to all the stakeholders.