The AML/CTF compliance transformation

Pascal Eber
Partner
Operations Excellence
& Human Capital
Deloitte

Bastien Collette
Director
Operations Excellence
& Human Capital
Deloitte

Adrien Chiariello
Senior Consultant
Operations Excellence
& Human Capital
Deloitte

Sarah Audrey Samou
Consultant
Operations Excellence
& Human Capital
Deloitte

Over the last few years, the compliance function has had to cope with heightened regulatory pressure. Compliance departments have grown in size, at increased cost to organizations. In addition, compliance departments must improve their efficiency and play a key role in implementing regulatory changes.

The time has come to transform the compliance function so that it can fulfil its primary roles, which include the oversight (monitoring and testing) of a company's activities. The corporate governance and culture of institutions need to change and this will involve making changes to the tools and services they use (technology, enhanced collaboration with external specialists, etc.).

Some institutions have already embarked upon this transformative journey by searching for efficient solutions and services so as to be compliant with all applicable rules.

The concept of compliance is frequently overlooked because it is seen as lacking any positive impact on business activities. Given that compliance is an *absolute* (i.e., it cannot be partially achieved), it is also seen as an overwhelming regulatory mountain to climb. In fact, since the concept of compliance is so pervasive, the best way to achieve compliance is to ensure compliance in every business activity and not consider it as a stand-alone topic or goal.

While hefty fines for regulatory misconduct far exceed the cost of efforts to ensure compliance, beyond the financial loss, non-compliance often has the following deeper impacts on businesses:

First, reputational risk: broadcasting a positive image has never been as hard as it is today. Ever since the emergence of now-ubiquitous communication technologies, customer awareness and protection have been growing in importance. On the top of that, fines and sanctions are now made public, which weighs heavily on the scales of public opinion.

Next, we have corporate culture impairment: bosses favor motivated employees united under one flag and one business purpose. This is what corporate culture is all about. Nevertheless, corporate misconduct, when detected, is usually an attempt at personal enrichment to the detriment of the company's wealth. When committed by senior executives, the cultural damage felt deeply by those on the bottom rungs of the ladder.

Avoiding regulatory misconduct requires more than mere procedures and well-trained compliance teams. The involvement of senior management is essential. Investing in compliance and the regulatory framework is no longer a box ticking exercise. It requires more dedication and qualitative resources to set up a process to ensure efficient and accurate compliance with constantly changing and increasingly stringent regulatory provisions.

Regulators do not expect financial institutions to merely comply with the rules; instead, they are called upon to be pro-active. This new challenge should motivate financial institutions to re-think how they go about investing in compliance.

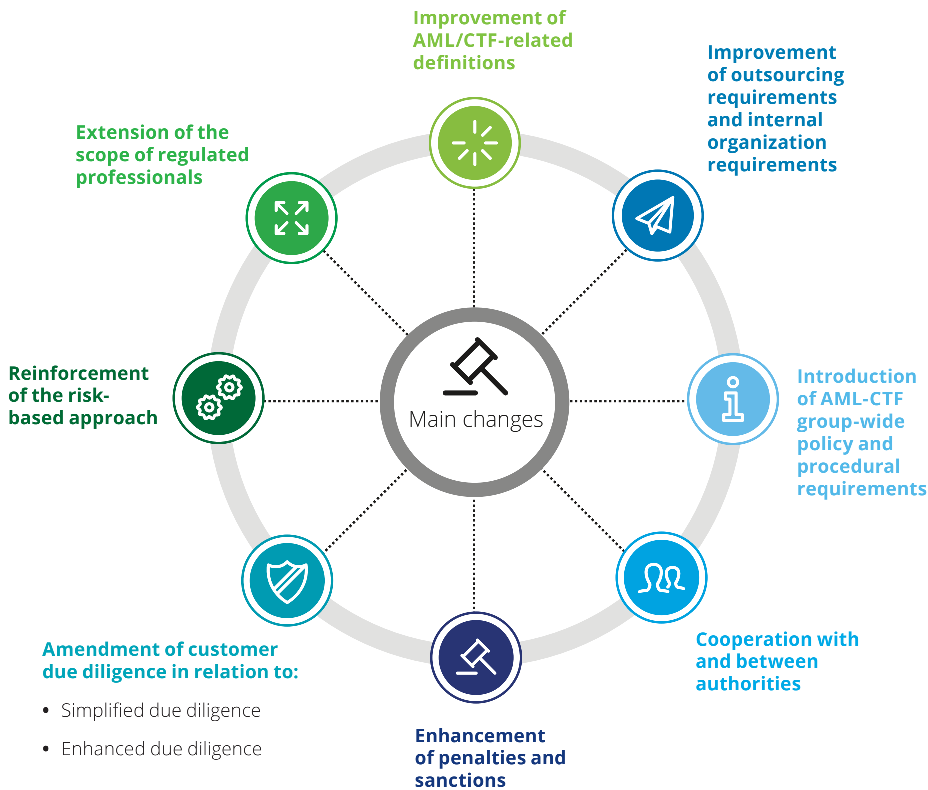
Obstacles to full compliance

Ever-increasing regulatory pressure

It would be impossible to argue that financial institutions have not faced a rising tide of regulatory pressure over the past 10 years. One of the reasons why this pressure can sometimes become unbearable is that these regulations rapidly evolve over time and expand in scope with every update. In the last 24 months alone, new acronyms have entered the lexicon of every compliance officer: AMLD IV, MiFID II, GDPR, etc.

Compliance departments must constantly adapt their policies, procedures, controls, and processes. AML/CTF laws and regulations are the perfect example of rapidly expanding scope. For instance, the Luxembourg law of 12 November 2004 relating to AML/CTF, as amended most recently in February 2018, follows on from the partial implementation of AMLD IV into Luxembourg law (which began with the tax reform and joint circular 17/650 of 17 February 2017 making tax crimes a predicate tax offence to money laundering).

The main changes brought in by this law are:



In this era of digital transformation, organizations that are slow to invest in proper IT infrastructure are denying themselves access to valuable data.

AMLD IV's full transposition into national law will be achieved when the national UBO registries for trusts and legal entities currently subject to separate transpositions (bills of law N°7216 and N°7217) become legally applicable Luxembourg.

AMLD V and VI are already being discussed at EU-level, and this is just the beginning

Face the real-IT-y

It has become difficult, if not impossible, to dissociate the increasing need for digital tools from the stricter requirements introduced by the new regulations. Financial institutions are used to investing vast sums in tools that serve the business—i.e., the departments that "create" money. FinTech has overwhelmed the financial market over the past decade with countless innovations revolutionizing the banking profession. The most recent wave of innovation has finally paved the way for technology dedicated to the regulatory framework itself. RegTech, as it is known, is technology created to enable financial service providers to fulfil their compliance obligations. Time will tell, but we may now be on the brink of a new era in terms of the digitalization of regulation.

The UK Financial Conduct Authority is considering developing machine-executable regulatory requirements to reduce the compliance burden on financial firms. Other jurisdictions including Singapore and Hong Kong are also taking the lead, encouraging companies to develop products in response to new financial regulatory requirements. The reality is that while RegTech is still growing, a lot of financial entities have yet to adopt compliance-friendly technology. Financial services companies may be reluctant to properly invest in such technology, as it is perceived as having the dual disadvantage of both costing money and not bringing in any income. In this era of digital transformation, organizations that are slow to invest in proper IT infrastructure are denying themselves access to valuable data. From an AML/CTF standpoint, this not only considerably hampers the detection of relevant alerts ("know your transactions")—also, in most cases, the quality of data drives resource allocation.

It is noticeable that data is often collected and stored purely for the sake of complying with regulations but rarely exploited once it has been buried in servers for years. Additionally, customer relationship management (CRM) and KYC systems typically require a significant amount of KYC information ("data") that is rarely embedded in the best way, leading to a disappointing front-end user and customer experience, as well as the risk of having, for instance, incorrect AML client risk scoring attributed, incomplete client and related-party information used for name screening, etc.

The brain shortage

Despite the regulators' strenuous efforts to make AML/CTF a serious subject, organizations are facing difficulties in hiring and retaining talented professionals, as evidenced by the plethora of job vacancies for AML/CTF specialists (we recommend that you check this on your favorite job search engine). If financial institutions have got the message, civil society has yet to catch on, since very few academic institutions seem to be providing a specialized AML curriculum or even teaching AML as a subject in its own right. Why are compliance officers not making a career out of their jobs? Well, maybe in part because when they are hired they currently have to struggle with outdated systems or spend a considerable amount of their time convincing other business lines and management of the importance of a new procedure from a compliance point of view. Down the road, the best talents seek new challenges in front-office positions or move to competitors offering higher salaries.

Compliance teams are often left frustrated by the challenge of performing their duties without the appropriate tools. This is compounded by the growing regulatory burden and the fact that, all too often, they are not properly integrated into the company's culture.

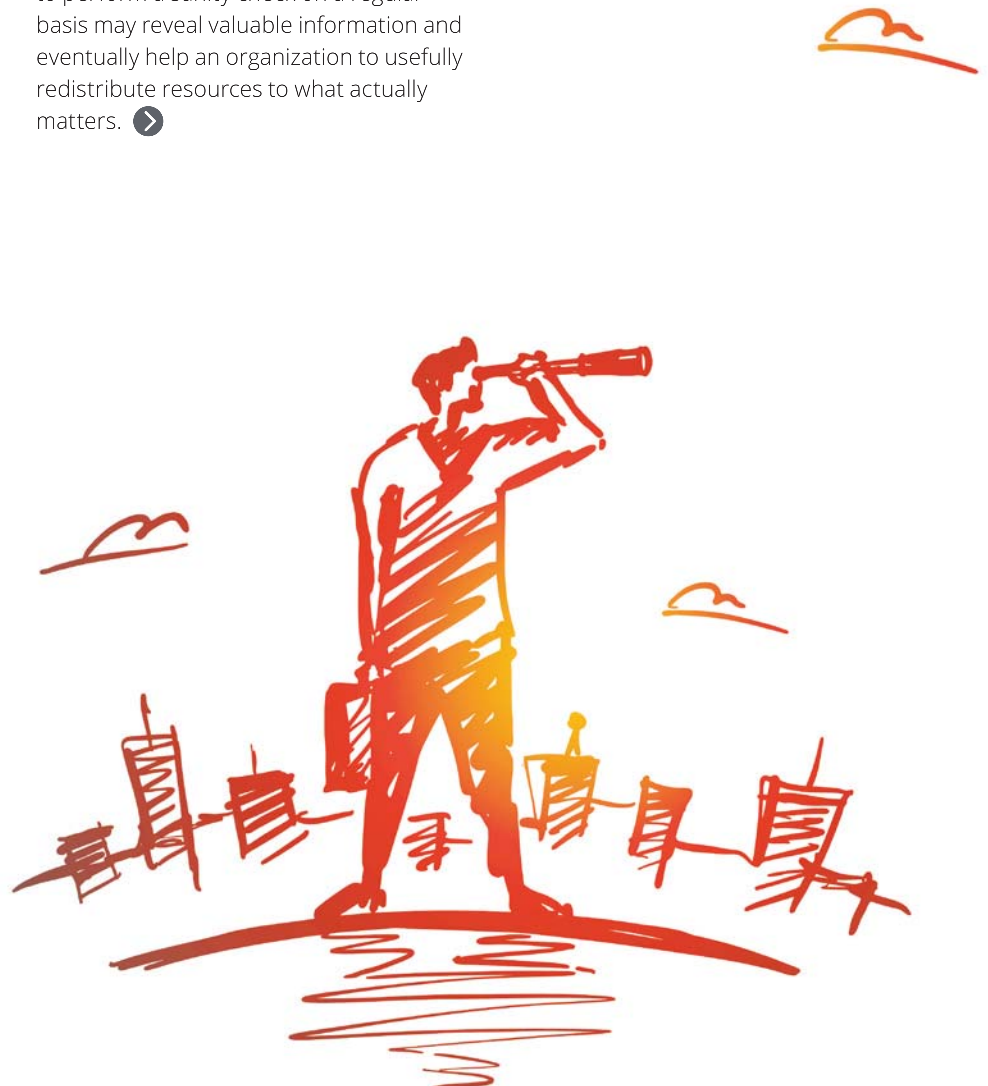
Streamlining the compliance framework

In light of these obstacles on the pathway to full compliance, organizations must undertake several essential steps[1] to initiate their compliance transformation.

Mind the gap

Few of us would be willing to set out on a long and important trip without getting our vehicle checked beforehand. A similar analogy could be applied to the compliance/AML journey. Moreover, it is twice as important because, in many cases: some chief compliance officers (CCOs) do not have the opportunity to be involved from the beginning in the construction of their own department, but instead have to manage a structure left by a predecessor or an interim CCO. Such situations can lead to inefficiencies in many ways: e.g., confusion between the responsibilities of the various lines of defense, poor coordination and reporting of exceptions, and even duplication of control activities or a failure to ensure proper oversight. Hence, asking independent third parties to perform a sanity check on a regular basis may reveal valuable information and eventually help an organization to usefully redistribute resources to what actually matters.

Compliance teams are often left frustrated by the challenge of performing their duties without the appropriate tools. This is compounded by the growing regulatory burden and the fact that, all too often, they are not properly integrated into the company's culture.



1 Non-exhaustive list

Empower the first line of defense
How many times have we heard compliance officers, when investigating a suspicious case, complain that if they had known all the facts from the outset they would not have allowed such a business relationship in the first place? This kind of event teaches us that the quality and timeliness of the information collection process is of paramount importance in the fight against money laundering. Thus, at the very beginning of the process, the front office must bear full responsibility for ensuring that, at the end of the chain, compliance gets the right information at the right time. Ideally, this communication stream should be a two-way street, with compliance providing regular, measurable feedback to front-office teams so that the latter have a clearer understanding of the importance of their actions. Unfortunately, this does not happen overnight. At times, we see that the front office and compliance do not have the best possible patterns of communication for the simple reason that they only have to talk to each other when something goes wrong. Changing this pattern may be arduous but it is an essential step towards continuous improvement.

Empirically biased
Compliance departments have a lot to gain from setting up adequate and accurate KPIs to monitor their activity and performing efficient sample testing. KPIs are part of the prudential control setup in most compliance departments, but there is ample scope to question their effectiveness. As mentioned earlier, relevant data will provide key insight into the efficiency of controls, and it will also serve as a basis for arguments to present before the board of directors and authorized management bodies regarding the provision of additional resources to ensure the compliance of the organization as a whole. To achieve this, compliance could present management with specific metrics that are important from a decision-making perspective, including sufficient details on the various business lines and client types, as well as on matters not directly linked to the business. In essence, a good KPI should pinpoint where the issue is coming from so that it is easier to take corrective action. The difficulty in identifying the right KPIs for compliance teams stems from how hard it is to quantitatively evaluate the full scope of their tasks. Establishing the right KPIs is no easy or short task, and no KPI should be set in stone over time, but successful KPI implementation will sharply increase the relevance and timeliness of compliance activities. Moreover, the growing number of (sometimes unpredictable) reports requested from regulators significantly adds to compliance departments' workload in a way that is not always measurable.

Prioritize the exceptions
On any given day, a compliance officer receives on average 200 alerts[2]. While this may sound like a crushing workload for anyone, we believe that only one fifth of these alerts actually deserve attention. The causes of this distortion include the aforementioned factors:

- Poor quality of data initially input because of inefficient systems and quality, and insufficient exhaustivity of information and documents received from the first line of defense.
- The first line of defense is not sufficiently held accountable or trained to detect missing or improper information during the on-boarding process.

That said, not all items in the vast swathes of data and alerts are equal or even require a due date. Considering the sheer volume of alerts to take care of, simply categorizing them could be a job on its own. Along with other broader considerations, this is why a risk-based approach to AML/CTF makes complete sense. Systems featuring embedded algorithms to sort through such a dataset are suitable for this, assuming they have been accurately configured in the first place and consider, for instance, the ML/TF risk attributed to each customer. The importance of having adequate KYT scenarios is essential. Compliance has to think ahead when deciding how best to design and implement effective AML/CTF detection rules based on scenarios rather than just thresholds. The growing interest in RegTech makes this the perfect time to refocus the prioritization of compliance duties. Embedding machines and tools would help reduce the number of false positives, for instance in the case of transactions monitoring, and it would enable compliance to focus on value-added analysis of false negative cases that previously went undetected.

Monitor, monitor, monitor
Many organizations have officers whose role it is to monitor the regulatory calendar and thereby ensure that the entity is thinking ahead. This is indeed highly important. However, how many organizations have set up a monitoring

2 The cost of compliance—2017, Thomson Reuters

structure to detect the potential failures and inefficiencies, regardless of tax regulations, of the compliance program itself? As a matter of fact, the most straightforward ratios are the best allies. For a minute, why not roughly estimate these metrics?

Take, for instance, the evolution of your customer portfolio ML/TF risk level, which will tell you a lot about your AML risk scoring. Or the staff attendance and success of AML-related training, which will probably give you an idea of the number of people you still need to inform of their AML/CTF obligations. How about the number of positive alerts (name screening, transaction monitoring and filtering) versus the number of items screened that could prompt a rethinking of the setup of transaction monitoring, name screening, and filtering systems. You could even estimate the size of the backlog of pending alerts, so as to allocate the right amount of resources to it.

As organizations move towards a full compliance program, there are ways to reduce the hassle of implementing all of the solutions needed to prevent money laundering.

- Leverage top-notch systems: this has become so trendy that RegTechs have made an industry of it, with solutions that are generally cheaper than developing in-house workarounds
- Take advantage of the experiences of industry experts: if you have faced a suspicious transaction, chances are that you are not the first potential victim, nor the only one. In many cases, even if the perpetrator is not the same, industry experts know of other cases with similar fact patterns, and hence are best placed to provide the right course of action
- Train your compliance staff regularly: on-the-job training is the best way to truly get to grips with what you should know. Nevertheless, eventually compliance officers will need to get a little taste of what they do not know, so that they are better equipped to handle new fact patterns as they arise
- Perform a data cleansing of your database and full monitoring of all tasks
- Outsource some of your AML/CTF activities to third parties so that your compliance officers can focus on their main oversight tasks

Compliance blossom

01 **Compliance focus**
- Reduce time on low value-added tasks
- Focus on main oversight

02 **Accurate monitoring**
- Monitoring of compliance duties
- Monitoring of non-compliance staff on regulatory matters

03 **Efficiency of the capital**
- Human capital (training, competencies of compliance staff)
- Financial capital (technology tools)

04 **Strengthening regulation**
- Growing and specific expectations from regulators
- Wider scope