A Work Project, presented as part of the requirements for the Award of a Master's degree in International Finance from the Nova School of Business and Economics.

A REVIEW OF COMPLIANCE'S DIGITALISATION IN THE FIGHT AGAINST MONEY LAUNDERING: AN ILLUSTRATION FROM DELOITTE'S LUXEMBOURG PERSPECTIVE

ROBERTO FERREIRA AUGUSTO

Work project carried out under the supervision of:

Pranav Desai

16/01/2023

Abstract:

Digital transformation is vital to compliance expansion and risk strategy development that match future technological requirements. Reviewing the scope under which digitalised processes' implementation evolves, this paper shows where compliance stands in the regulation's technological revolution and the opportunities and challenges associated. Data management, heavy costs, lack of talent and a difficult cultural shift are just a few of the explanations for why it is among the last to hear about digitalisation. While improving efficiency, lowering costs, and increasing transparency are all critical components in its fruition. The results are eventually illustrated through a current proposed solution by Deloitte Luxembourg.

Keywords: Anti-Money Laundering, Compliance, Digitalisation, DKYC, Deloitte Luxembourg, KYC, Digital Technology, Financial Crime, Regulation

This work used infrastructure and resources funded by Fundação para a Ciência e a Tecnologia (UID/ECO/00124/2013, UID/ECO/00124/2019 and Social Sciences DataLab, Project 22209), POR Lisboa (LISBOA-01-0145-FEDER-007722 and Social Sciences DataLab, Project 22209) and POR Norte (Social Sciences DataLab, Project 22209).

Table of Contents

Table of Figures

1. Introduction

Since the global recession of 2008, regulatory requirements and the demands placed on compliance by supervisory bodies have grown drastically in the financial industry. From the immediate reaction after the Great Recession with the implementation of The Dodd-Frank Act in 2010 (Forbes, 2022) to the latest AMLD6 in Europe in 2021 (European Commission, 2021), passing by the numerous updates made on the Bank Secrecy Act in the last fifteen years (FinCEN, n.d.), these standards mainly were addressed for a long period by dedicating additional resources to compliance.

However, technological advancements and pricing pressures have the potential to drive alternate solutions that will eventually become permanent. Financial institutions can answer to regulatory pressure more effectively thanks to digitalisation. The potential increases in efficiency and effectiveness will significantly reduce the criterion for profitable investments in compliance operations. With the increase of speed in the movements of financial transactions and the new technologies, money is being transferred all around the globe with ease as never before, with, for instance, remittances reaching $630B in 2022 (World Bank, 2022). Thus, the technology in the domain regarding the fight against money laundering must keep up with that pace.

The first line of defence used worldwide against financial crime is compliance measures, notably in financial firms. From The Global True Cost of Compliance 2020 report of LexisNexis, the predicted global financial institutions' combined cost of financial crime compliance was €187.6 billion in 2020, up from €160.5 billion in the previous year. In the financial place of Luxembourg, for instance, the banking sector spent an average of €630k on AML in 2020, while the typical percentage of banking employees that work on regulatory matters was up to 13.9% (EY-ABBL, 2020). The cost of maintaining regulatory compliance is significant. Switching back and forth between different systems and platforms can create inefficiencies in time management and raise risks. Automation may therefore enhance the working experience and cut costs as regulatory compliance is maintained.

This study examines the scope within which the implementation of digitalized procedures grows, as well as the potential and problems related to the regulatory technology revolution. Also, a unique chance to get an inside view of an actual solution developed by Deloitte Luxembourg is presented to provide an overview of what a centralized all-in-one digitalized tool looks like.

A wide range of materials will be used to be able to compose this master's thesis. Various terms and concepts will be defined by reviewing a variety of literature, analysing a variety of reports and research, looking at case studies, investigating some AML solutions, and discussing the current state of compliance and its anticipated developments. Online books, reports from well-known businesses and organisations, leading firms in the domain of financial crime, and some pieces from reputable news sources are only a few of them. The whole list of references may be found at the bottom of this essay, and among them are reports and articles from the Financial Action Task Force (FATF), EY, EUROPOL, Deloitte, Forbes, the OECD, the World Bank, some Luxembourgish journals and others like Forbes, the United Nations Office on Drugs and Crime (UNODC), LexisNexis, Thomson Reuters or the European Central Bank (ECB).

2. Literature review

As mentioned before, many sources and mainly statistics on the topic of financial crime can be found within renowned organizations in the field, but also some relevant papers tackled some questions about regulation and technology. For instance, (Arner et. al., 2016) suggest that the revolutionary character of technology will only be grasped by a new strategy that lies at the nexus of data, digital identity, and regulation. Indeed, the role of regulators is key, and because of the dispersion of market actors and the rising use of technology, regulators must implement a sequential reform process, beginning with digitization and progressing to digitally-smart regulation. This procedure is outlined in the article of (Zetzsche et. al., 2017). Regulators must also build a robust new framework that supports innovation and market trust, helped by the deployment of regulatory "sandboxes" (Arner et. al., 2017). Because of the wave of new legislation that followed the 2008 financial crisis, (Colaert, 2017) investigated the frequently overlooked issue of how financial institutions may remain compliant with this constantly developing financial legal system. On the AML side, a noticeable paper by (Tiwari et. al., 2020) looked at the state of research in the domain of money laundering and concluded that the sensitive matter regarding shell companies is a highly under-explored field, with great potential for further research and opportunity to help the fight against financial crime.

3. Background on AML and Regulation

Anti-money laundering

The matter of money laundering is taken very seriously and for a very simple reason: it is estimated by the UNODC that between 2 and 5% of global GDP – representing between €700 billion and €2 trillion – is laundered each year. Recently terrible scandals shook the world. For instance, the €200 billion laundered through an Estonian branch of the largest bank in Denmark, Danske Bank, from 2007 until 2015 (Bjerregaard and Kirchmaier, 2019). But money laundering dates almost as long as money itself exists. Already in ancient Asia, money laundering schemes have been discovered where merchants wanted to hide their wealth from governments, or in the Middle Age when moneylenders were involved in various systems to cover up illicit practices, as well as later pirates disguising the origin of their loot (Gelemerova, 2008). And it is during the United Nations (UN) Vienna 1988 Convention that money laundering is described in its Article 3.1 as: *“the conversion or transfer of property, knowing that such property is derived from any offence (s), for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in such offence (s) to evade the legal consequences of his actions”.* The process of money laundering normally involves three steps (placement, layering and integration) before the money is eventually released into the legitimate financial system. Nowadays, advances in technology and the increased availability of complex financial products and transactions have led to increasingly sophisticated money laundering techniques.

Regulation

Following the focus put on the matter by the UN in 1988, it resulted in a series of regulations being put in place regularly up to our days at the international, European, and country levels. The global and regional standards-setting bodies to mention only a few, are the FATF, Egmont Group, International Monetary Fund (IMF), World Bank, UNODC, and Basel Committee on Bank Supervision. But they are all observer organizations of the FATF; indeed, the latter is the pioneer in matters of financial crime worldwide. This inter-governmental body, established in 1989 by the Ministers of its Member jurisdictions, has as a purpose to establish international standards and develop and promote policies both at national and international levels, to combat money laundering and terrorist financing. FATF is considered to be a policy-making body which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas. A year after its establishment, it issued its first set of 40 Recommendations, significantly influencing the coming regulations in Europe over the past thirty years. In fact, in 1991, Europe sees its first Anti-Money Laundering Directive (AMLD), responding to a vital international approach in the fight against financial crime. The member states would then implement the directive's obligations into their national law as they intended to, but as an objective to have a common ground and minimum requirements. The first directive also called 1AMLD, aimed at those countries to criminalize money laundering. Followed in 2001 2AMLD, expanding the predicate offence definitions to be aligned with the FATF. 3AMLD, in 2005 brought an additional topic to the table, including the issues related to terrorist financing, while 4AMLD, ten years later in 2015, widened the scope of AML rules to comprise Designated Non-Financial Businesses and Professions (DNFBPs) such as gambling entities. A few three years later, 5AMLD included a notion today of the up-most importance of Ultimate Beneficiary Owners (UBOs), requiring more transparency in the economical ownership of entities. Most recently, the latest directive, 6AMLD, was published to add 22 predicate offences to the current ones, including environmental and cybercrimes. Further, in July 2021, the European Commission (EC) unveiled a comprehensive set of legislative measures to strengthen the EU's AML/CTF regulations. According to the European Commission: "*This package is part of the Commission's commitment to protecting EU citizens and the EU's financial system from money laundering and terrorist financing. This package aims to improve the detection of suspicious transactions and activities, and to close loopholes used by criminals to launder illicit proceeds or finance terrorist activities through the financial system.*" This incoming novelty will be integrated with the creation of a new supervisory authority for AML in the EU financial sector called the Anti-Money Laundering Authority (AMLA) (Consilium, 2022).

4. Compliance

A comprehension of compliance

As just seen, regulations and other guidelines are set by organizations and agencies. But all directly aim for the same thing: influencing and obliging the firms falling under its scope to comply with measures in an attempt to lower financial crime. Nevertheless, the reality is not as simple as just having some employees apply some rules to comply with regulatory requirements. And this domain is called Compliance. Often seen as the less glamorous and interesting department of a firm in comparison with Sales or Product Development, for instance, it is still one of the most important without which a business could not run. It refers to corporations following governmental laws and regulations that the firm is subject to, as well as internal policies. But compliance is not just a legal requirement; it must be seen as the minimum to keep its operations safe and threats from outside (Investopedia, 2020).

In addition, it must encompass expectations from all stakeholders affecting the firm and keep on an ongoing basis any effort to satisfy their needs. Every single facet of an organization is impacted by compliance and regulates the daily tasks of every employee. The latter takes another level, particularly in the financial world. The crisis of 2008 will remain forever in society's thoughts, and regulators specifically. After the incident, financial compliance turned out to be the number one concern and a serious matter to be never left aside. It is also a necessary tool to preserve public confidence in the banking industry and capital markets. Since the latest global crisis, the accent was put on transforming the teams from solely advising compliance to actively having a risk-based management approach. The role of compliance can be resumed into 5 areas of responsibility, namely identification, prevention, monitoring and detection, resolution, and advisory. Therefore, in addition to the threat of imprisonment and fines, the latter list of duties is one of the most important lines of defence in the fight against financial criminality.

The due diligence process

The fight against financial crime covers topics, not exhaustively, from terrorist financing, corruption and bribery, fraud, and market abuse, to money laundering. AML/CTF has been a particular point of attention lately, as seen before on an international stage, and no country is exempt from it. But how does the compliance department of financial services firm fight this criminality? The goal of any entity will be to avoid any problem before it becomes a reality, thus, prevention is key. The threats of fines and public shame from regulators are also what fuels this willingness to prevent. The ambition is to decrease the risk and guide the company into the best market practices. The crucial step in fighting money laundering and preventing dealing with any consequences related to it is mainly encompassed within the scope of what is called due diligence (DD). It aims at identifying, assessing, preventing and mitigating risks associated with the counterparties identified. The challenge within DD covers especially, but not only, sanctions screening, politically exposed person (PEP) identification, alerts resolution, customer risk profiling and onboarding, and regulatory reporting. It is all about gathering information on who/what the financial institution is dealing with, at any level, current or potential, internal and external to the firm. Each demand for information should be cautiously proportionate to the risk the counterparty brings.

The DD is the most important part of the well-known broader standards of know your customer (KYC). KYC is an essential step for a financial firm in its AML operations before entering into business with any counterparty. It all begins with conducting risk-based processes, which involve taking rigorous onboarding measures and acquiring all counterparty information required to assess the possible risk of doing business. The type of information needed to be gathered depends on the counterparty the firm is dealing with, but as basic data, one can mention identities, addresses, names, activities, sources of funds, related parties, and other specific lists of relevant documents. Counterparty risk must be assessed, analysed, and scored. However, if a prospective client has a higher risk potential during this due diligence journey, extra steps requiring a deeper risk analysis are implemented. As a result, the primary purpose of this AML phase is to analyse all potential risks associated with conducting business with the targeted counterparty and, consequently, measure a customer's ability to commit financial crime. Regrettably, even though financial firms are substantially investing in their KYC procedures, many of these procedures are still highly manual and have several opportunities for improvement. KYC procedures are ideal candidates for digital transformation since they are filled with manual, repetitive operations, elevated work volume, and rule-based choices that raise the likelihood of mistakes.

Challenges

On paper, it seems like everything is ready to be applied, and some good compliance officers would do the job. But financial institutions face increasing challenges within their KYC strategy and operations, compelling them to think and act differently. Challenges range in a variety of aspects. The never-ending stream of new and updated anti-financial crime regulations, bringing each time its surplus of complexity, is constantly challenging the teams. The lack of talent within the firms is leading to a very strong demand for efficiently managed resources. The costs related to compliance are of the utmost importance and are one of the main elements adding pressure, demanding more and more decrease of spending in back-office functions. In fact, after a survey of over 300 of the UK's leading financial institutions, it revealed an average annual AML compliance cost of £186.5 million, with up to £300 million or more for larger entities, for which 70% of the budget was spent on acquiring, training, and keeping employees, with slightly under 25% spent on tech (data, solutions, and systems) (LexisNexis, 2021).

But at the same time, there is a need to increase resources for technology to keep up with the ongoing business. The place of financial crime compliance mostly relies on as an influencer in the onboarding processes while the front office is doing the main tasks as the first line of defence. An appropriate shift in the model is inevitable but comes with its load of own challenges. It is then, on one side, a need for increased operational efficiency with a cost increase, onboarding time, and a constantly evolving regulatory environment, and on the other side, a need for increased risk management with the pressure from supervisory bodies, controls and sanctions, and the financial risk and reputational damage (Thomson Reuters, 2021).

Compliance with AML, KYC and sanctions requirements continue then to be an ongoing focus area for financial institution management, and businesses must make sure they are adhering to the proper compliance practices. Keeping track of legislative changes still need a lot of human work in compliance processes, which is time-consuming, prone to error, and expensive. And despite the recent efforts, compliance and risk management are frequently still viewed as separate concepts. New technologies gave criminals' hands an infinity of possibilities to commit their crimes. In today's rapidly changing world, compliance offices are sometimes still operating with old procedures and being limited by too much manual work. Also, companies must balance the cost of compliance and its complexity while keeping in mind the experience for their customers. Maintaining compliance is nowadays more than just satisfying the supervision bodies. The rising demand for digital from users constantly challenges institutions and put pressure on the risks that must be managed (Forbes, 2021). Today firms must face a revolution in their compliance processes if they are willing to keep up with the pace. The multitude of regulatory requirements is leading financial institutions towards efficient solutions, fast processes, cost-improving methods and quality in the treatment of the data.

Where are we with digitalisation in compliance?

Companies are researching methods to better manage compliance expenses in a world where security concerns are essential. Increased spending on anti-money laundering solutions might result in additional benefits, which can offset the negative consequences of fraudulent operations. It is now over a decade that the financial industry put the accent into using technologies to enhance experiences for its customers, but only more recently has it shifted the focus also onto its operational side (Thomson Reuters, 2021). None can deny the great impact of digital transformation in several areas, and it was time to put eyes on compliance. The growth of compliance and the creation of risk programmes that satisfy future technological requirements both depend on digital transformation. Companies cannot afford to ignore their risk and compliance responsibilities in an environment that is becoming more regulated. In response, businesses are giving their risk management specialists more authority and better tools and today's technology is one of the most crucial instruments available to the risk function. The AML solutions in the market nowadays are differentiated at various levels. First, by the targeted domain (KYC, compliance reporting, transaction monitoring, or auditing), then there are two types (services or software), the way it is implemented (on-premises or on-cloud), and geographically (Mordor Intelligence, n.d.).

But why are compliance and, more broadly, risk functions being the latest to find out about digital transformation? The answers stand for a variety of reasons, but three important angles might be mentioned. First, senior management often sees digital transformation as a way to only grow customer relationships and the business. Functions and departments directly impacting P&L see a transformation because of their clear return on investment. Compliance and other internal functions, such as audits, end-up being last impacted by it. Second, such functions might not yet be aware of the pace and extent of digitalisation happening within the company. Or, if they are tuned in, they can perceive technology's potential to alter or even replace them and see it as a threat rather than an opportunity. Third but not least, under weak management, the focus of IT might be turned too much to other parts of the organization and leaving the transformation of some departments behind (Deloitte, 2020).

Still, companies are facing numerous other challenges also, mainly, as mentioned earlier, budget constraints. The latter was deeply accentuated after the pandemic, which left several scars. And another matter of great consideration is the fast-evolving regulation environment, threatening the companies in their right choice of software. Indeed, the challenge for any firm is being able to pick the right fintech resources that will not be obsolete two years later (KPMG, 2017). Following both last pieces of challenges mentioned, other areas identified are also a pure lack of in-house skills, confidentiality and data protection, prevention from strategic management and no understanding of the potential of such solutions, or poor IT infrastructure. One can also add two additional areas that might impact such transformation, namely operational resilience and regulatory acceptability.

Benefits of digitalisation in compliance

New technological solutions in compliance are then clearly seen as a mandatory path that must be taken by companies. As discovered formerly, the constant growth in regulatory compliance requirements makes digitization and its use unavoidable. And this shift is supported by many benefits, and some were already mentioned earlier. But some key components emphasise the future role digitalisation will take within compliance offices. Moreover, tackling these issues eliminates one of the most significant risks for compliance, which is having a considerable amount of data but failing in using it (NorthRow, 2022).

Better tools for more accurate analysis of customer relationship monitoring ensure that possible trouble situations may be discovered much more promptly. Also, manually retrieving information from disparate systems that are not linked together, on the other hand, takes a significant number of resources and time. The expenses of digitization can be offset by the savings in potential misbehaviour prevention and manual process substitution. Furthermore, digital solutions enable financial institutions to anticipate changing client behaviour, allowing them to differentiate themselves from their competitors. Plus, to avoid being harmed by the upcoming financial sector consolidation, all financial institutions must replace all repetitive operations and resource-intensive sectors with digital solutions. Another winning point for firms is the quality of insights they can gather. Improving them is advantageous since such proactive, real-time monitoring may enable improved identification and mitigation of systemic hazards. Also comes the matter of transparency. Indeed, better quality data enables more transparency and better decision-making and enhances monitoring capabilities, making it possible to concentrate on the decision-making process and risk assessment (NorthRow, 2022).

Financial institutions are beginning to recognise digitization and automation as opportunities to gain a significant business advantage by cutting costs and guaranteeing complete regulatory compliance. And eventually, by automating and digitising operations, the sector may not only successfully manage compliance risks and lower related costs but also enhance service quality.

An article from Refinitiv in 2019 highlighted the benefits specifically of KYC and came out with numbers to the extent to which proper KYC-managed services may save a financial institution between 35 and 60% of the cost of conducting the function in-house.

5. Real example put into practice: DKYC by Deloitte Luxembourg

DKYC origin and Deloitte Luxembourg

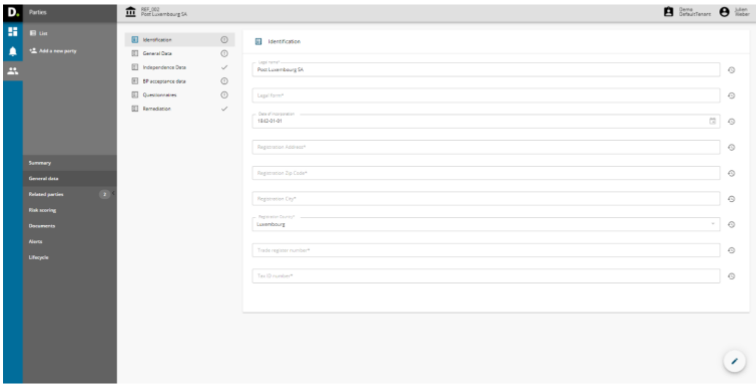
Challenges of digitalisation financial institutions are facing are of special importance in one specific place in Europe, the Grand-Duchy of Luxembourg. A unique environment where all the matters of regulation play a key component. Geographically in the centre of Europe and a legal hub, Luxembourg is one of the most important financial places in the EU and worldwide. The widespread use of English, French and German significantly improves connections between investors and the market worldwide and with a wide variety of financial services. It is the second biggest investment funds hub in the world after the US, and the country saw a surge in private equity firms choosing to establish their base of operations there. This environment, accompanied by competent and varied professionals in the financial sector and a high degree of stability in various domains, led to money from all around the globe coming through its frontiers. Even if the country holds the title of smallest land and population size in the EU, the fund industry found there a cocoon to develop itself with unprecedented speed in the last decades. Net assets under management in Luxembourg funds amounted to approximately EUR 874 billion in 2000, and it went up 10 years later to almost EUR 2.2 trillion, and in the year 2021, even hit EUR 5 trillion mark in January (Annex 5). The sustainable growth is mainly due to the very big appetite for Undertaking for Collective Investment in Transferable Securities (UCITS). Funds are part of the identity of Luxembourg, but it brings with them all the necessary baggage of compliance around it. Deloitte Luxembourg well understood the opportunity of implementing a suitable solution in this financial centre. It knew how to combine its advisory expertise with the right technology to provide a unique competitive advantage. DKYC, for Deloitte Know Your Counterparties, is an all-in-one service that combines numerous KYC features and workflows with AML/CTF expertise. The service is supported by a multi-channel and web-based platform and allows their clients to delegate, optionally, the execution of predefined KYC activities to Deloitte. In addition to using its DKYC solution for its clients and other counterparties, this solution satisfied a wide variety of demands coming through the financial sector, which are elaborated more in detail after the illustration. Asset managers use it for their KYC on assets of private equity and real estate deals but also their distributors and service providers, corporate banks, and law offices on their clients, but also all kinds of asset servicers required such processes on their investors, as well as support for remediation plans of private banks. DKYC is available in three alternative modes of delivery to accommodate any company or counterparty profile. As a platform, DKYC is installed on the customer's premises and is solely controlled by client personnel; as a hosted platform, it is housed by Deloitte and entirely handled by client personnel; and third, as an operating model, hosted by Deloitte and is operated by client personnel covering both operational tasks and validation/management decisions while Deloitte operators are entitled solely to operational tasks.

A journey into a DKYC process

DKYC is an all-in-one and end-to-end KYC platform, and in the following part, it will be shown in practice how new technology can help by going through each important step of a KYC journey. One of the main advantages DKYC possesses is its ability to adapt to any situation. And that is why the first step when any new client adopts the solution is to tailor the tool up to every detail to be in accordance with its risk-based approach. Every individual approach to risks is implemented within DKYC and sets up the basis of the tool, the matrix. In addition, several workflows may be designed for onboarding, offboarding, and periodic review at the discretion of the company. Throughout the implementation process, these procedures are evaluated and set up, and they may be rapidly altered during production. According to the intended operating model, an indefinite number of phases (including approvals) can be assessed while considering many criteria (e.g., type of counterparty, current due diligence level, a specific event, user role/permission, etc.).

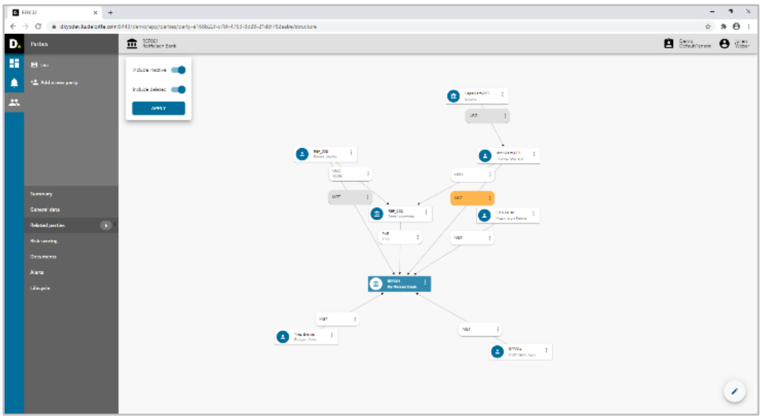
Comes then the start of any due diligence process regarding a new counterparty the firm is entering into business with (investors, new clients, services providers, assets, etc.) by collecting the necessary information. DKYC can keep a predetermined list of fields/questionnaires for the counterparty (i.e., the subject of the KYC file) and its associated parties. For example, the list and character of the fields can be tailored to the established risk-based methodology. Furthermore, fields can be organised in a variety of ways, and DKYC will save a complete data history for each field.

Figure 1 - Collection & input of counterparty static data according to the predefined risk-based approach:



An important feature comes next, which is determinant in better understanding the big picture around the KYC target. A dynamic graph is nowadays indispensable to catch the story going on around the asset being evaluated and of critical importance when one is dealing with very complex structures, such as Trusts or multi-layered structures. It is possible to add/maintain as many "related parties" as necessary for each counterparty, including one or more roles (from a pre-set list, going from the directors to UBOs passing by banks involved in the deal) and static data. This makes it simple to enter and maintain a structured picture of the counterparty ownership structure, which includes intermediaries and other responsibilities based on unique counterparties (e.g., private clients, vendors, service providers, investors, distributors, alternative assets, etc.).

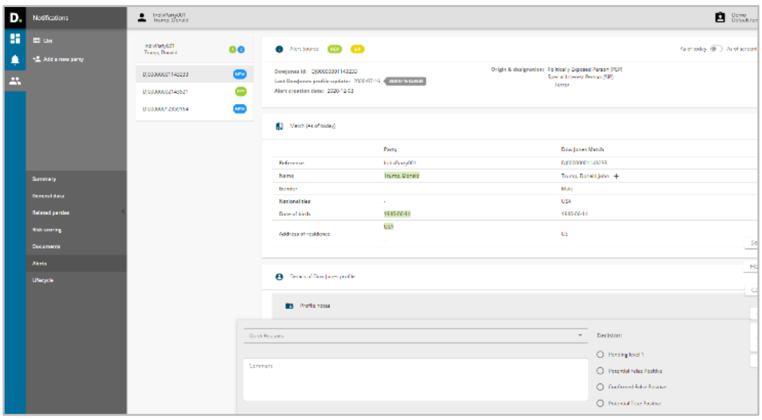
Figure 2 - Materialized ownership in a structured manner:



© 2022 Deloitte Solutions SàRL (PSF)

The notion of screening and alert management is another key feature and essential to any KYC process. Therefore, DKYC uses Neterium JetScan (advanced name screening technology), DowJones Risk & Compliance (market leading watchlist for sanction/official lists, PEP and their relatives, Special Interest Profiles), and DowJones AME (Adverse Media Entities) to conduct automated Watchlist screening in real-time at onboarding and daily thereafter. DKYC incorporates all these elements entirely and smoothly. As a result, alarms are handled directly in DKYC, and underlying choices have an immediate influence on the risk level of the current KYC file.

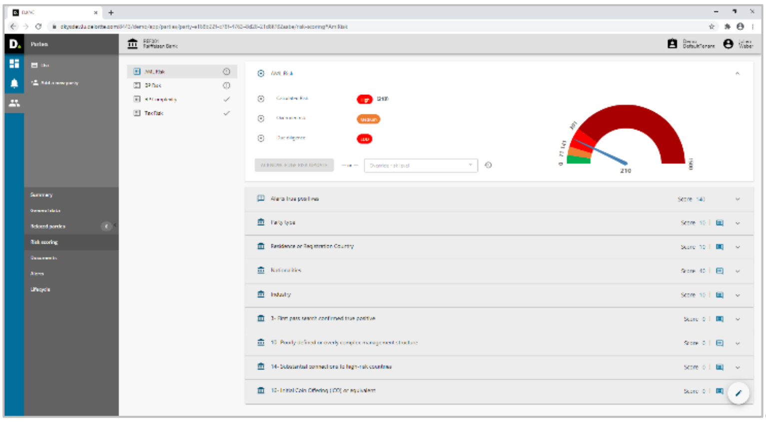
Figure 3 - Automated and real-time name screening on all stakeholders; incorporated case management; automated feed of alert choices to risk calculation:



© 2022 Deloitte Solutions SàRL (PSF)

As mentioned earlier, the goal of such due diligence procedures is to assess the risk being faced with a new counterparty. Since such a core element, the risk environment was then made clear and fully integrated into the solution. DKYC will calculate and maintain a risk score (and hence a risk level and due diligence level) for each counterparty in real-time, based on a pre-set list of risk criteria specified in accordance with the risk-based approach used, which will automatically adapt the required list of documents to be gathered for the counterparty. By default, the risk model is based on conclusions reached on watchlist screening warnings. Each alert category (for example, sanction, official list, PEP, PEP associate/relatives, special interest person, adverse media, etc.) might contribute a unique score to the model. Furthermore, allowed users can override a calculated risk threshold to deal with unique scenarios, requiring a comment to keep evidence of the manual operation performed and the override recorded for audit trail purposes.

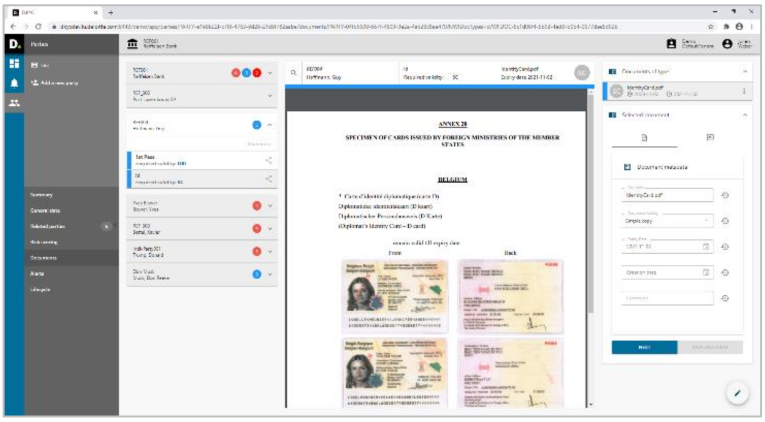
Figure 4 - Automated risk computation:



© 2022 Deloitte Solutions SàRL (PSF)

A great time-consuming task in any KYC is related to document management. For each onboarding or periodic review, or any other work performed, the effort in gathering the right documents and documenting it is one of the biggest points of improvement available. This is, therefore, why DKYC has an incorporated and dynamic document management feature that depends on the kind of counterparty and the current value of due diligence. It enables the upload, qualification, and maintenance of documents as well as their metadata. DKYC additionally keeps track of each document's state (missing, uploaded, qualified, outdated, etc.) and expiration date (if any).

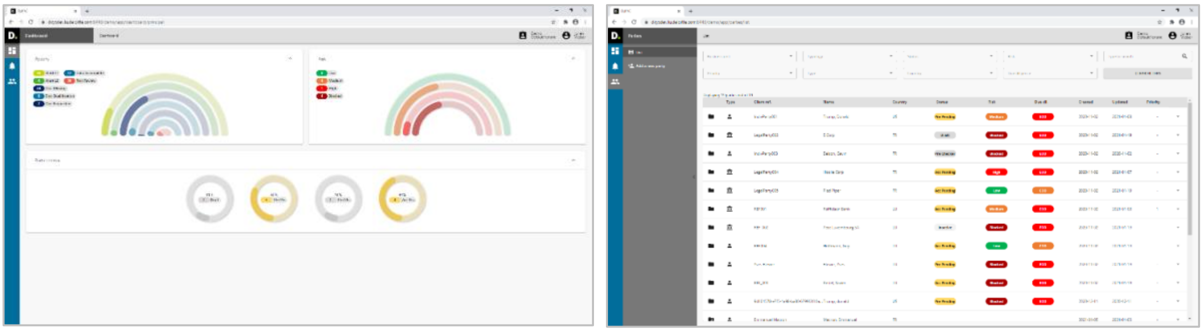
Figure 5 - Collect, input and qualify KYC documents dynamically according to the type of counterparty and the due diligence level:



© 2022 Deloitte Solutions SàRL (PSF)

Furthermore, it provides ongoing due diligence through automated risk scoring, name screening, monitoring of changes of circumstances, the trigger of periodic review, and real-time KPIs and reporting. The whole solution is also enabling an automated notification system when a manual action is needed on a file and offers a strong audit trail.

Figures 6 & 7 - Ongoing due diligence and automated notifications:



© 2022 Deloitte Solutions SàRL (PSF) *© 2022 Deloitte Solutions SàRL (PSF)*

Finally, the platform offers a wide range of choices regarding report generation for any purpose, from any statistical needs to external and internal audit requirements.

Why is DKYC a proven winning solution

The DKYC service has been running for over 3 years and delivering a tailored solution for stakeholders of the Luxembourgish financial place. Over 15 companies, including leading corporate and private banks, along with leading management companies and asset services, rely on DKYC to build/maintain KYC files on various counterparty types within their banking and investment management value chain. The success of such a service relies mostly on the fact the Deloitte team tackled the main challenges that were being encountered. It resolves the issues of extensive use of emails and paper that were making traceability difficult, eliminates some redundant activities that were leading to inefficiencies, it efficiently manages data to avoid inconsistencies and duplication of information, implements clear workflows, and weak audit trails are things from the past. Any firm developing software in this domain must bring updates in some key details that Deloitte targets at its best. The clients benefit from improved data quality and traceability, the onboarding time of counterparties is reduced, and internal resources of the compliance team can focus on core activities and essential controls. Moreover, in the rough battle of solutions' competition, one can notice specific aspects Deloitte and other firms with the same environment can use to their advantage. Nowadays, it is demanded more than just providing a tool, but also to know how to add some specific added values. Strong arguments for an entity like Deloitte to play a key role in winning the market, like being a service operated by a regulated and supervised entity in Luxembourg, assure confidentiality and treatment of data. But also, the vast network of senior experts and a previous long experience in AML/CTF are an asset for precious advice and management of complex cases, which simple tech companies cannot provide. Also, in addition to centralizing all the KYC processes in one tool solely, which other providers offer nowadays too and with great digitalisation, it goes further and implements robust ongoing monitoring, which is essential. This all-in-one tailored solution for KYC process and files management is a truly versatile tool, and its ability to provide adaptability to any kind of assets a KYC must be carried out on, from individuals to complex financial schemes, passing by alternative investments is its true strength.

6. Reflection on the current state and future outlook

Current situation

After the overview of such benefits a right implementation can have, the transition into more digital tools in compliance seems inevitable. And the governments - more precisely, the supervisory bodies - will certainly soon establish mandatory requirements for financial institutions to accelerate the digital transformation. Both recent events having worldwide impacts also contributed to an obliged change in the mindset of management concerning compliance. The impact of COVID-19 showed the world how vulnerable a company being behind in terms of technology can be. Processes of onboarding in KYC turned out to start being fully online, and a quick adaptation to these distant methods obliged the entities to revolutionize their operating models. This kick did good to accelerate the transition and awakened many minds still reluctant to get on board. Distant and digitalized processes are now key requirements, and any company going against that wind is bound to lose market share. The other major event that opened the eyes of the reductants to see a radical needed change in the way to approach regulation is the war in Eastern Europe. The sanctions against Russia coming from western jurisdictions at a never-seen speed is the perfect example of how things can turn tricky in an instant, and the right tools to be ready to face such a “regulatory mess” is of importance number one, having strong screening methods in place is definitely essential in this period.

Growth opportunities drive digital transformation, which is followed by rising market pressure as well as new regulatory requirements. It is the procedure of evolving to new digital processes to boost productivity and stay up with market needs. Organisations are evolving from a transactional model to a more complex interaction between individuals and the automated devices and systems they employ.

Future

The rapid growth of fintech during the last two decades brought a lot of novelty in various domains and revolutionized daily actions. Even though compliance and regulatory functions are part of the ones being the last getting up to speed with it, it was not completely left aside by everyone. The rising interest in crypto money and its blockchain environment also got into regulation, and some leads on how the use of this revolution could help certainly have its part to play in the future. The KYC context has been studied along blockchain, and some interesting directions are to be noticed. Some of the current issues mentioned earlier with the processes most companies have in place nowadays are being targeted by blockchain solutions. The problems of accuracy, access, storage and veracity of the data, a central element of KYC, are being addressed by elaborated techniques solvable by employing blockchain technology as a mechanism of storing KYC data. When a financial service firm does a KYC check on a specific counterparty, the KYC statement and all essential information are stored on a blockchain and may be viewed by other institutions and recognised businesses. This eliminates the need to initiate the entire KYC procedure, lowering administrative expenses and workloads. Furthermore, because information recorded on a blockchain is irreversible owing to its nature, it would constitute a single and dependable source of truth. Customers will only be required to submit their KYC files once when using this upcoming technology since all other establishments will rely on blockchain verification. It might look futuristic, but it's great to see some engagement, and it is by looking for already that smaller steps will be taken. It is the example in Luxembourg of the partnership between Fundsquare, a fund data and documentation provider established there, and i-Hub, a fintech subsidiary of Groupe POST Luxembourg specialising in KYC services, together going in the same direction as the previous example with centralization and sharing access as the main focus. The solution offers a highly secure, global digital KYC repository. It allows for the interchange of documents and data, as well as the gathering, verification, validation, lifecycle management, and digital storage. It also gives both financial and non-financial businesses and their consumers a multi-terminal link to KYC data and documents. The process removes the necessity for establishments and their clients to supply numerous copies of papers, decreasing risk and inefficiency dramatically. It also makes collecting client paperwork easier, resulting in considerable operational savings.

Nevertheless, the such approach brings its load of challenges and has not yet gained the full confidence of the Luxembourg fund industry. In an era where data is at the centre of attention, especially in Europe, it is being confronted with problems of data confidentiality and in terms of responsibility.

Limits and risks of going digital

Some points have been detailed previously already regarding the implementation of digital tools, but the last few words opened the door directly to other limits the digitalisation of compliance is facing. As just mentioned, data is one of the key components of this revolution. And one aspect at the centre of debates is true regarding the transparency and access to it, more particularly targeting the concept already evocated before, UBO. The 4AMLD was the first directive to establish requirements regarding entities' beneficial owners. More transparency was requested, and it led the EU to each country to create a register of financial beneficiary owners. Dependent on the country, access to the data is more or less public and restricted (annexe 2). In Luxembourg, the "RBE" was fully accessible to the public, and anyone could have their hands on data on the beneficial owner, including residential address. In November 2022, after a complaint from a Luxembourgish-based executive, the European Court of Justice decided to definitely restrict this access globally in the EU on the grounds of privacy regarding the sensitive aspect of the data available (PWC, 2022). It is a step back in the continuous effort of transparency in the fight against money laundering in Europe. It poses the question of the trade-off between the availability of data for a better fight against financial crime and data privacy and transparency. These concerns are indeed embedded in a larger scope regarding data in general. The digitalisation of compliance management is under the scrutiny of cyber security, privacy and improper data integration.

But the biggest challenge might not come from the technology itself but rather the human side of the coin. Culture is one of the key concepts in that and plays an essential part in this revolution (PWC, 2019). Digitalisation and improvements to reduce risks come with a heavy process for the compliance teams, and companies may overlook some cultural elements. They will need to strategize the implementation of new approaches. The company's overall digitization aspirations must be matched with the digital establishment of compliance services. The role of technology can only be fully realised if it is entrenched in a programme that involves everyone on the digital journey: a cultural shift and acceptance at all degrees. The most difficult challenges are frequent in people's thoughts.

Another barrier, coming from an angle already touched, is the cost. The heavy investments in digitalisation can be outweighed by the cost of paying fines for non-compliance with AML/CTF regulatory requirements. The question of the worthiness of such implementation is often on the table. It is why some countries like Luxembourg recently changed their approach and started to publicly announce the fines imposed on companies, which was kept mostly secret in the past, nowadays to threat with "name-shaming" and its consequences that can be way bigger than direct financial ones.

Finally, on the technical side, some words can be mentioned on the boundaries it encounters. Indeed, many solutions are present on the market, but one of the main challenges for a company is to find the right tool for its needs. The adoption of an unsuitable product by a firm could have serious consequences. In addition, extensive use of very advanced technology like machine learning (ML) and artificial intelligence (AI) for compliance is still facing its very big stop, respectively, being able to provide a fully comprehensive audit trail. Choosing ML/AI still comes with its undesirable "Blackbox". Also, a difficulty still present in the eyes of many concerning it is being able to conceptualize the idea that compliance officers doing a lot of paperwork going through a sudden change and becoming fully knowledgeable in using blockchain and advanced technologies.

7. Conclusion

The digitalisation of compliance is at a turning point. Many opportunities for improvement at all levels are possible, and the range of options is wide. But it was also understood that such transitions must be taken care of cautiously and in line with human and technological limits, as well as financial ones. Also, in certain cases, the persistent perception of compliance as "cost centres" rather than "strategic business centres" may dominate, causing delays in getting started. Companies must exhibit a clear commitment to how technology will revolutionise the compliance requirements within the firm to effectively digitise the compliance process. A solid risk management culture and a firm tone from senior management, governance and oversight are much than ever required. Proper compliance software are also crucial in making sure that the compliance operating model addresses critical concerns and that it encompasses future changes and challenges (business, operational and technological ones). After automating what can be automated, enabling collaborative work is key. Success usually relies on the implementation of the right process and tools, enabling an effective collaboration between the teams and a strong single point of truth in terms of KYC, for example. Effective communication across multiple disciplines like compliance, IT, audit, data analysis, and the front office is one element for success. But it is also critical to reduce management's inappropriate expectations. The return on investment must be clearly defined and analysed ahead of time. Long-term cost savings are linked with digitalisation. As already stated in 2009 by former U.S. Deputy Attorney General Paul McNulty, "*The cost of non-compliance is great. If you think compliance is expensive, try non-compliance.*" (Compliance Building, 2009). Not to add the worth of quality improvements, which is sometimes significantly higher. Both may and should be used to justify management's investment in digitalisation. Compliance would have more time for essential responsibilities, such as qualitative examination of data that has been collected and classified digitally. This elevates the prominence and importance of compliance.

8. References

"AML/CTF – DKYC." Deloitte Luxembourg. Accessed December 2022. https://www2.deloitte.com/lu/en/pages/financial-advisory/solutions/deloitte-kyc.html.

"Anti-Money Laundering and Countering the Financing of Terrorism Legislative Package." EC, July 20, 2021. https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en.

"Anti-Money Laundering Market Size Report, 2021-2028." Anti-money Laundering Market Size Report, 2021-2028. Accessed December 2022. https://www.grandviewresearch.com/industry-analysis/anti-money-laundering-market.

"Anti-Money Laundering Solutions Market Size, Share 2022 - 27." Anti-Money Laundering Solutions Market Size, Share 2022 - 27. Accessed December 2022. https://www.mordorintelligence.com/industry-reports/anti-money-laundering-solutions-market.

"BSA Timeline." BSA Timeline | FinCEN.gov. Accessed December 2022. https://www.fincen.gov/resources/statutes-regulations/bank-secrecy-act/bsa-timeline.

"Cutting the Costs of AML Compliance." Oxford Economics, March 22, 2022. https://www.oxfordeconomics.com/resource/cutting-the-costs-of-aml-compliance/.

"Digital Transformation for the Risk and Compliance Functions: Deloitte Us." Deloitte United States, March 3, 2020. https://www2.deloitte.com/us/en/pages/advisory/articles/digital-transformation-risk-compliance-functions.html.

"Digital Transformation: What Does It Mean for Compliance?" ComplySci, September 30, 2020. https://www.complysci.com/blog/digital-transformation-for-compliance/.

"Fintech, Regtech, and the Role of Compliance Report 2021." Thomson Reuters. Accessed November 2022. https://legal.thomsonreuters.com/en/insights/reports/fintech-regtech-compliance-report-2021.

“Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010” EUR-Lex. Accessed November 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0421.

“Money Laundering.” United Nations : Office on Drugs and Crime. Accessed November 2022. https://www.unodc.org/unodc/en/money-laundering/overview.html#:~:text=%E2%80%9Cthe%20conversion%20or%20transfer%20of,legal%20consequences%20of%20his%20actions%E2%80%9D.

“New Eu Authority for Anti-Money Laundering: Council Agrees Its Partial Position.” Consilium, June 29, 2022. https://www.consilium.europa.eu/en/press/press-releases/2022/06/29/new-eu-authority-for-anti-money-laundering-council-agrees-its-partial-position/.

“Remittances to Reach $630 Billion in 2022 with Record Flows into Ukraine.” World Bank, May 11, 2022. https://www.worldbank.org/en/news/press-release/2022/05/11/remittances-to-reach-630-billion-in-2022-with-record-flows-into-ukraine.

“Report: Cutting the Costs of AML Compliance - LexisNexis.” Accessed December 2022. https://solutions.risk.lexisnexis.co.uk/cutting-the-costs-of-aml-compliance.

“Research: Tech Blockers 2022 – Cutting the Costs of AML Compliance.” FinTech Futures, November 17, 2022. https://www.fintechfutures.com/2022/11/research-tech-blockers-2022-cutting-the-costs-of-aml-compliance/.

“Statistics.” ALFI. Accessed November 2022. https://www.alfi.lu/en-gb/annual-report/2020-2021/statistics.

“Survey on the Cost of Regulation and Its Impact on the Luxembourg Financial Centre.” EY

Luxembourg. Accessed November 2022. https://www.ey.com/en_lu/banking-capital-markets/survey-on-the-cost-of-regulation-and-its-impact-on-the-luxembour.

"The New Horizon for Anti-Money Laundering Solutions." Capgemini, August 12, 2022. https://www.capgemini.com/insights/expert-perspectives/the-new-horizon-for-anti-money-laundering-solutions/.

"True Cost of Financial Crime Compliance Study Global Report." LexisNexis Risk Solutions. Accessed November 2022. https://risk.lexisnexis.com/global/en/insights-resources/research/true-cost-of-financial-crime-compliance-study-global-report.

"What Is Compliance? [Definition & Examples Guide]." ERM Software, April 7, 2022. https://www.logicmanager.com/resources/grc/what-is-compliance-guide/.

"What Is Customer Due Diligence (CDD)?: Swift - the Global Provider of Secure Financial Messaging Services." SWIFT. Accessed November 2022. https://www.swift.com/your-needs/financial-crime-cyber-security/know-your-customer-kyc/customer-due-diligence-cdd#:~:text=In%20the%20world%20of%20Financial,a%20customer%20or%20potential%20customer.

"What the Tech?! #11 - Regtech." Homepage. Accessed December 2022. https://digital-luxembourg.public.lu/stories/what-tech-11-regtech.

Arner, Douglas W. and Barberis, Janos Nathan and Buckley, Ross P., The Emergence of Regtech 2.0: From Know Your Customer to Know Your Data (January 1, 2016). (2016) 44 Journal of Financial Transformation 79, UNSW Law Research Paper No. 17-63

Arner, Douglas W., Janos Barberis, and Ross P. Buckley. "Fintech and Regtech in a Nutshell, and the Future in a Sandbox." CFA Institute, July 1, 2017. https://www.cfainstitute.org/en/research/foundation/2017/fintech-and-regtech-in-a-nutshell-and-the-future-in-a-sandbox.

Bjerregaard, Elisabetta and Kirchmaier, Tom, The Danske Bank Money Laundering Scandal: A Case Study (September 2, 2019). Available at SSRN: https://ssrn.com/abstract=3446636, or http://dx.doi.org/10.2139/ssrn.3446636

Calin. "History of Anti Money Laundering Directive: A Summary - Part One." ComplyAdvantage, August 25, 2022. https://complyadvantage.com/insights/brief-history-amlds-part-one/.

Cornelius, Doug. "McNulty Keynote on a Tale of Two Sectors." Compliance Building, June 4, 2009. https://www.compliancebuilding.com/2009/06/04/mcnulty-keynote-on-a-tale-of-two-sectors/.

Gelemerova, L. Y. (2011). "The anti-money laundering system in the context of globalisation: A panopticon built on quicksand?" Wolf Legal Publishers (WLP).

Gelemerova, L. (2008). "On the frontline against money-laundering: the regulatory minefield." Crime, Law and Social Change, 52(1), 33-55

Greggwirth. "Cost of Compliance Report 2022: Officers Face Competing Priorities & Future Planning." Thomson Reuters Institute, July 6, 2022. https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/cost-of-compliance-report-2022/.

Hargrave, Marshall. "Compliance Department: Definition, Role, and Duties." Investopedia. Investopedia, October 30, 2022. https://www.investopedia.com/terms/c/compliancedepartment.asp.

Lafferty, Catherine. "Fundsquare and Fintech Firm to Launch KYC Utility." Funds Europe. Accessed December 2022. https://www.funds-europe.com/news/fundsquare-and-fintech-firm-to-launch-kyc-utility.

Lone, Shakeel. "ServiceNow Brandvoice: The Creeping Cost of Compliance." Forbes. Forbes Magazine, April 21, 2022. https://www.forbes.com/sites/servicenow/2021/10/21/the-creeping-cost-of-compliance/?sh=38263cc256cc.

"Money Laundering." Europol. Accessed November 2022. https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/economic-crime/money-laundering.

NorthRow. "The Future of Compliance: Digital Transformation Meets Regulation." NorthRow, September 26, 2022. https://www.northrow.com/blog/the-future-of-compliance-digital-transformation-meets-regulation/.

Pearson, Lucinda. "Transparency International Urges EU to Act on Patchy Beneficial Ownership Registers." Transparency International EU, May 27, 2021. https://transparency.eu/eu-must-act-beneficial-ownership-registers/.

PricewaterhouseCoopers. "Compliance Benefits from Digitalisation." PwC. Accessed November 2022. https://www.pwc.ch/en/insights/risk/future-of-risk-2019/compliance-benefits-from-digitalisation.html.

PricewaterhouseCoopers. "News - Temporary Suspension of the Luxembourg RBE's Data Consultation." PwC. Accessed December 2022. https://www.pwclegal.lu/en/publications/temporary-suspension-luxembourg-rbe-data-consultation.html.

PricewaterhouseCoopers. "The Anti-Money-Laundering Package 2021 - 'Strengthening the Framework'. What's New?" PwC. Accessed November 2022. https://www.pwc.lu/en/newsletter/2021/aml-package-2021.html.

Schizas, Emmanuel and McKain, Grigory and Zhang, Bryan Zheng and Garvey, Kieran and Ganbold, Altantsetseg and Hussain, Hatim and Kumar, Pankajesh and Huang, Eva and Wang, Shaoxin and Yerolemou, Nikos, The Global RegTech Industry Benchmark Report (June 30, 2019). Available at SSRN: https://ssrn.com/abstract=3560811 or http://dx.doi.org/10.2139/ssrn.3560811

Smith, Kelly Anne. “How the Dodd-Frank Act Protects Your Money.” Forbes. Forbes Magazine, August 16, 2022. https://www.forbes.com/advisor/investing/dodd-frank-act/#:~:text=The%20Dodd%2DFrank%20Act%20was%20a%20law%20passed%20in%202010,by%20insurance%20companies%20and%20banks.

Tiwari, M., Gepp, A., & Kumar, K., A review of money laundering literature: the state of research in key areas (March 20, 2020). Pacific Accounting Review, 32(2), 271-303. https://doi.org/10.1108/PAR-06-2019-0065

Tuefekci, Ertugrul. “Digitalization as an Opportunity - Assets.” Accessed December 2022. https://assets.kpmg/content/dam/kpmg/ch/pdf/digitalization-opportunity-compliance-matters-en.pdf.

Walker, Gareth. “The Cost Benefits of KYC Managed Services.” Refinitiv Perspectives, August 12, 2019. https://www.refinitiv.com/perspectives/financial-crime/the-cost-benefits-of-kyc-managed-services/.

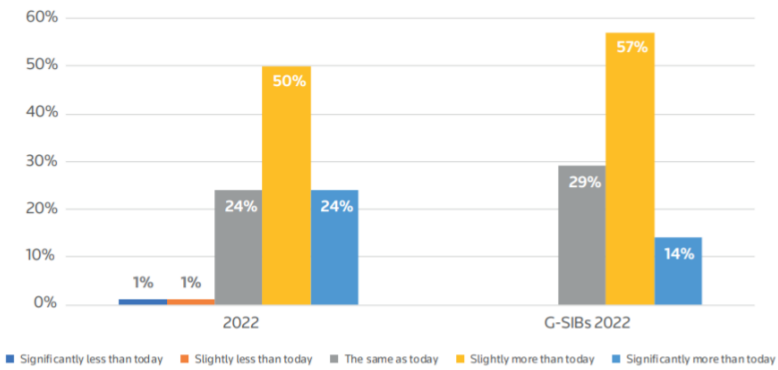
Zetzsche, Dirk Andreas and Buckley, Ross P. and Arner, Douglas W. and Barberis, Janos Nathan, Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation (August 14, 2017). 23 Fordham Journal of Corporate and Financial Law 31-103 (2017), European Banking Institute Working Paper Series 2017 - No. 11, University of Luxembourg Law Working Paper No. 006/2017, University of Hong Kong Faculty of Law Research Paper No. 2017/019, UNSW Law Research Paper No. 17-71, Center for Business and Corporate Law (CBC) Working Paper Series 001/2017.

9. Annexes

1. The figures and graphs below come from the annual report being conducted by Thomson Reuters in 2022, "Cost of Compliance Report 2022: Officers Face Competing Priorities & Future Planning". Nearly 500 practitioners from around the world responded to questions, representing global systemically important banks (G-SIBs), banks, insurers, asset and wealth managers, regulators, broker-dealers, and payment service providers.

Annexe 1.1: *The greatest compliance challenges I expect to face in 2022 is/are...*

Annexe 1.2: *Over the next 12 months, I expect the amount of regulatory information published by regulators and exchanges to be....*

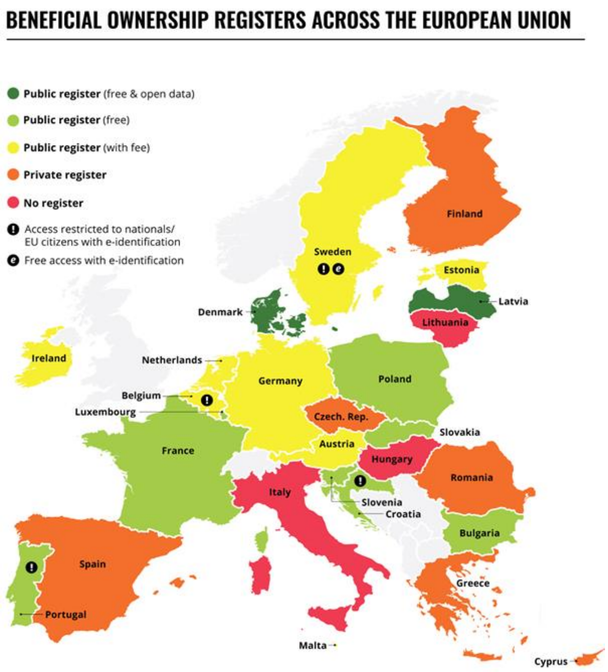


Annexe 1.3: *What are the three key skills required for an ideal compliance officer in 2022?*

Annexe 1.4: *What does the ideal future of the compliance function look like?*

Annexe 1.5: *The greatest compliance challenges the board expects to face in 2022 is/are*

Annexe 2: *This image provided by Transparency International reflects the progress of the implementation of the EU anti-money laundering directive across the Union in the matter of beneficial owner register.*

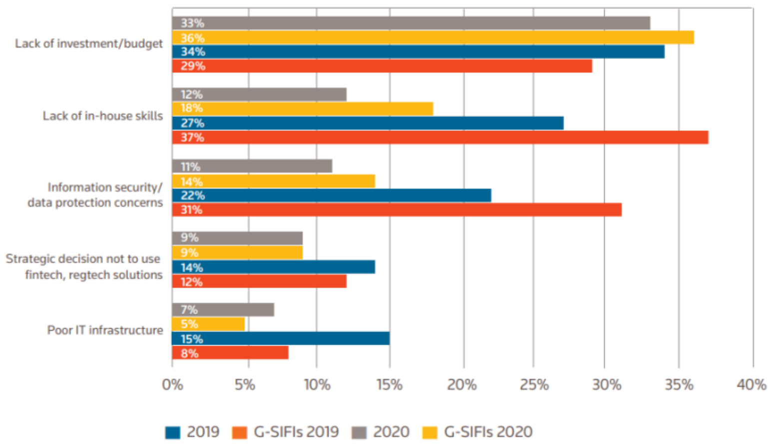


3. The figures and graphs below come from the annual report being conducted by Thomson Reuters in 2021, "Fintech, Regtech, and the Role of Compliance Report 2021". The survey results represent the views and experiences of more than 400 compliance and risk practitioners.

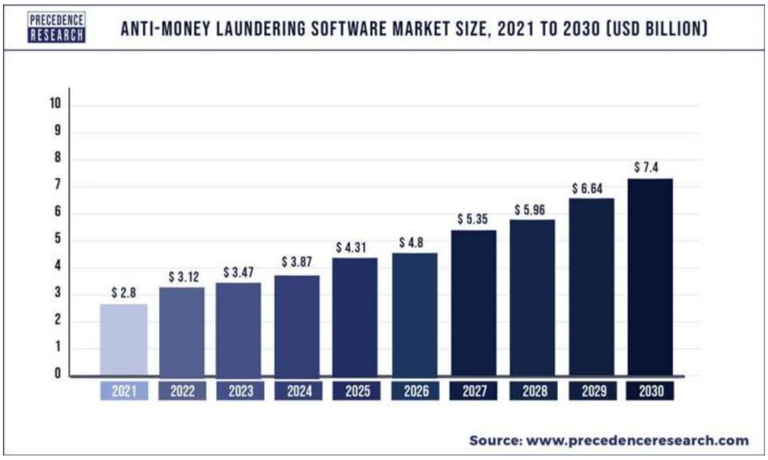
Annexe 3.1: *What solution have you introduced/ are in the process of introducing and to meet what compliance needs?*

Annexe 3.2: *The greatest benefits you expect your firm to see from financial technology in the next 12 months are…*

Annexe 3.3: *If your firm has not yet deployed fintech or regtech solutions, what is holding you back?*



Annexe 4: *AML market, 2021 to 2030 (https://www.precedenceresearch.com/anti-money-laundering-software-market)*



Annexe 5: The growth of the funds' industry in Luxembourg, illustrated by a graph coming from the annual report 2020-2021 of ALFI (Association of the Luxembourgish fund industry) https://www.alfi.lu/getmedia/5f1629f6-ca56-4afd-ab43-57e4d69970cc/alfi-annual-report-2021-2022.pdf

Net assets under management in Luxembourg funds