Capgemini invent

KYC & AML BENCHMARK STUDY 2022

Contents

01. EXECUTIVE SUMMARY

The importance of compliance has been underlined in the last decade through the multibillion fines issued on both sides of the Atlantic to financial institutions. Since then, the compliance function has always found itself at the intersection of two major lines of thought: on the one hand-side, objectively viewed, compliance is a pure cost center. On the other hand, it is also characterized by the famous saying, "If you think compliance is expensive, try non-compliance"[1] as proven by the hefty fines issued by the regulators. Both viewpoints are valid. Therefore, it is of paramount importance for financial institutions (FIs) to achieve efficiency in their compliance processes.

To what extent do FIs succeed in implementing efficiency levers, and how does the digitization state of the organization abet those levers? In this benchmark study, we examine the current state of financial crime compliance by focusing on the know your customer (KYC) and anti-money laundering (AML) processes. We focus primarily on the digitization state and the efficiency level of the surveyed FIs, and derive specific points of action from which the industry can benefit.

Key findings with regards to KYC:

- Large size banks steer their portfolio risk with >90% low-risk clients, reducing their KYC review workload
- There is a significant difference between regulatory requirements and actual review cycles
- More than half of surveyed FIs are facing customer complaints with respect to KYC – not fostering customer experience
- The manual workload is the most significant pain point within KYC processes
- The potential of technology is not even close to being exhausted, with the use of main "technology" being limited to automated client screening

Key findings with regards to AML:

- The banking industry still suffers from very high transaction monitoring false positive ratios – on average, 92%
- The degree of tool customization does not have a determining influence on the false positive ratio of transaction monitoring alerts
- The proportion of suspicious activity reports (SARs) as a percentage of transaction monitoring alerts is very heterogenous among the participating banks
- The vast majority of banks regard their AML process as cost-efficient despite very high false positives ratios
- In total, 50% of respondent banks regard themselves as only moderately digitized or not particularly digitized
- The potential of AI & intelligent automation is currently largely untapped but is expected to be at the forefront of technology investments in the next two years

[1] former U.S. Deputy Attorney General Paul McNulty

02. INTRODUCTION

Financial institutions face growing costs for the remediation of their KYC clients and the investigation of alerts for anti-money laundering, especially for the numbers of deployed employees, to handle their compliance processes, while the technology to support automation continues to evolve rapidly. Against this background, FIs must approach financial crime compliance with a clear strategy informed by the state of regulation and technology. Considering this, this benchmark study explores the current state of financial crime compliance and the opportunities for using innovative technologies.

03. MAIN

Concept & survey details

This KYC & AML benchmarking study assesses compliance efficiency and digitization state in the banking sector based on different KPIs. The study respondents are senior decision makers in the area of KYC and AML from selected leading European banks.

This report presents the findings of a survey on financial crime compliance conducted in 2021 & 2022 by Capgemini Invent. The conducted survey consists of qualitative and quantitative parts.

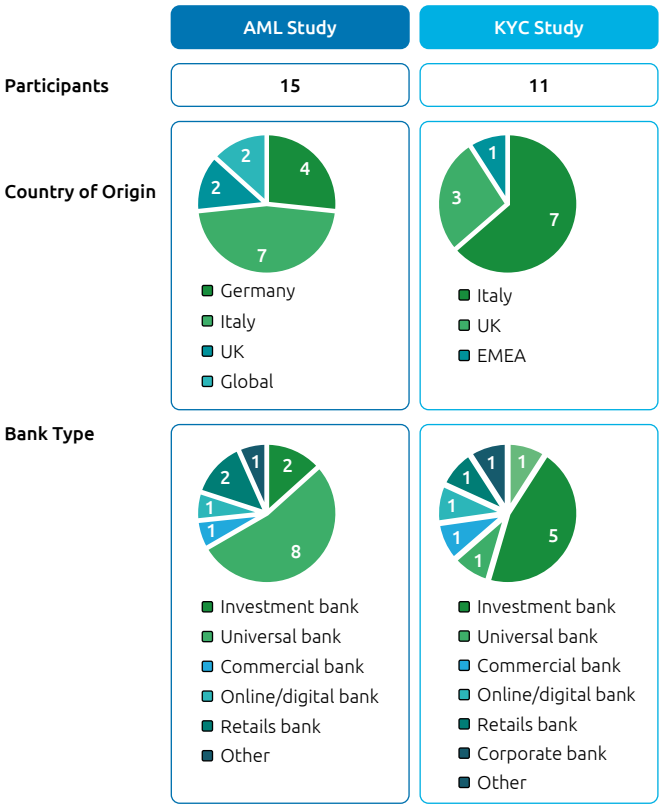
Main thesis & methodology

- Focus group: Leading European[2] banks, regardless of client profile (retail vs. corporate) and distribution strategy (digital-only vs. online & offline)
- Respondents: The interviewees were decision-makers within the compliance function of leading banks, i.e., chief AML officers/responsible parties for anti-financial crime initiatives
- Survey structure: Two questionnaires—based on the KYC and AML processes, and consisting of qualitative and quantitative parts—were presented to the study respondents
- Type of survey questions: The majority of the survey consisted of closed-ended questions structured along a Likert-type scale
- Answers: Answers that were apparently wrong/not meaningful were taken out of the survey to avoid falsifying the overall results
- Results interpretation: All results are interpreted anonymously; names of respondent banks are non-disclosable

Study

We asked more than 30 European banks about the efficiency of their AML & KYC processes. Among them, 14 responded to AML and 11 of them were about KYC.

Figure: 1 Overview of KYC & AML benchmarking study's participants



[2] We focused on European banks incl. also foreign banks operating through their subsidiary in the European continent. This way we ensure comparability of the figures delivered by the different institutions as AML regulation in all these countries is derived predominantly from the 6th AML Directive.

The AML respondents are predominantly Universal banks (8), followed by Retail (2), Investment (2) and Commercial (1) as well as Digital (1).

Similar distribution is observed amongst KYC respondents: approximately half are Universal banks (5), followed by equal parts Retail, Corporate, Commercial, Investment, and Digital banks.

We gathered insights on banks with different structures, ranging from small local banks to international financial institutions. We grouped the respondents in three buckets according to the size of their client portfolio – the key information points can be observed below:

Figure: 2 Overview of KYC & AML benchmarking study's participants

Characteristics	Max	Median	Average
Employees	230,000	12,400	36,716
Clients	50.000k	3.900k	9.650k
Natural Person Clients	20.000k	2.185k	5.200k
Legal Entity Clients	1.500k	228k	449k
Low Risk Client	4.100k	1.235k	1.691k
Medium Risk Client	150k	45k	57k
High Risk Client	75k	16k	24k
False Positive Ratio	99%	97%	94%
Cases per year	40,000	6,500	11,458
SAR filed per year	25,000	5,400	7,917
SAR based on TM*	100%	27%	36%
FTEs in AML	360	69	139

In total, we asked approximately 60 questions, 30 questions per AML & KYC questionnaire each, and some questions were identical in both questionnaires, such as concerning bank structure and digitalization.

Based on the results of all participants, we compared the data to gain insights about the effectiveness of the compliance organization. We looked at the relationship between different KPIs to conclude, for e.g., whether there is a positive relationship between the number of compliance employees and the number of risky clients, or whether there is a negative relationship between the number of alerts and the investment done on technology/digitization.

Another interesting analysis is the correlation between the percentage of false positives and the amount of AML compliance costs. Furthermore, the connection between the perceived digitization state, the percentage of false positives, and the allocated manpower to compliance processes is another focus area of this benchmark study.

* TM stands for "Transaction Monitoring".

APPENDIX 1: KYC detailed results

Financial institutions face growing costs for the remediation of their KYC clients. Especially the number of employees in their compliance processes increased, while the technology to support the automatization continues to evolve rapidly. Against this background, FIs must approach financial crime compliance with a clear strategy informed by the state of regulation and technology. Considering this, this benchmark study explores the current state of financial crime compliance and the opportunities for using innovative technologies.

Large size banks steer their portfolio risk with >90% low-risk clients, reducing their KYC review workload

The total number of clients of the surveyed financial institutions varies from 14 million to 7,5 thousand. The financial institutions have "on average" over 3 million clients. These clients are distributed in three categories: low-, medium- and high-risk clients. We took the total number of clients in each risk category concerning the overall clients. On an average, financial institutions categorize 93% of their clients as low-risk, 5% as medium-risks, and 2% as high-risk. We also found a positive correlation between financial institutions with fewer clients categorizing their overall clients with higher risks. In our survey, no financial institution with more than 200 thousand clients had a low-risk ratio of below 90%.

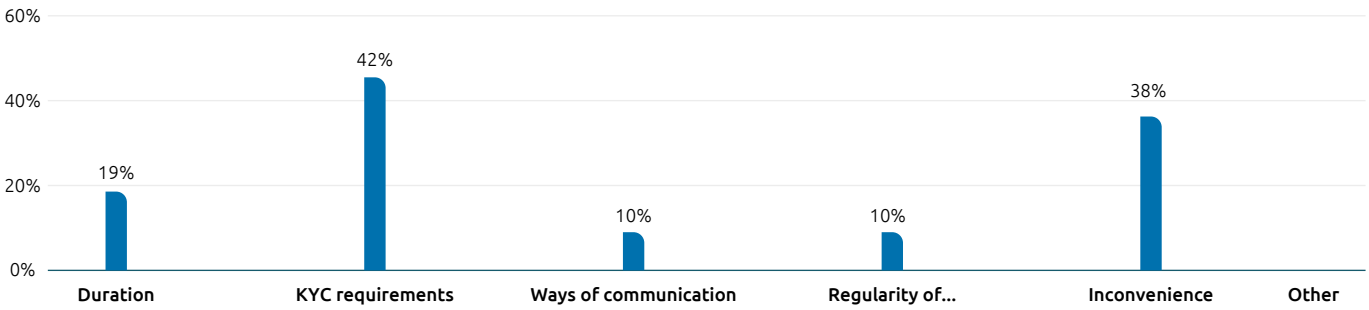
The reason, therefore, can be two-fold: larger financial institutions might have a stronger incentive to keep their risk ratings lower as the large numbers of client/KYC reviews will require excessive operations, or the larger financial institutions achieve client portfolio diversification with respect to not only credit but also KYC risk; whereas smaller financial institutions might have a stronger relationship with their fewer clients. Alternatively, the focus of smaller private banks might be on business areas that are more specialized and riskier, containing international clients or politically exposed persons that are classified as high risk.

There is a large difference between regulatory requirements and actual review cycles

The distribution of risk clients and the review cycles influence the FTE requirements for KYC operations. The review cycles vary from one financial institution to another, starting at 5 years to ending at 10 years for low-risk clients, with an average of 7.4 years. Medium-risk clients are being reviewed on an average every 2.8 years whereas high-risk clients require the shortest review period of only 1 year.

The process of creating a first-client KYC profile, called New Client Adoption (NCA), takes from 15 minutes to 3 hours for low-risk clients. Financial institutions estimate 45 minutes to 8 hours for medium-risk clients, and for high-risk clients, the average is about 25 hours. The shortest time required to onboard a high-risk client is 4 hours, while the longest is 80 hours.

Figure: 3 **What reasons do customers state if they complain about KYC?**



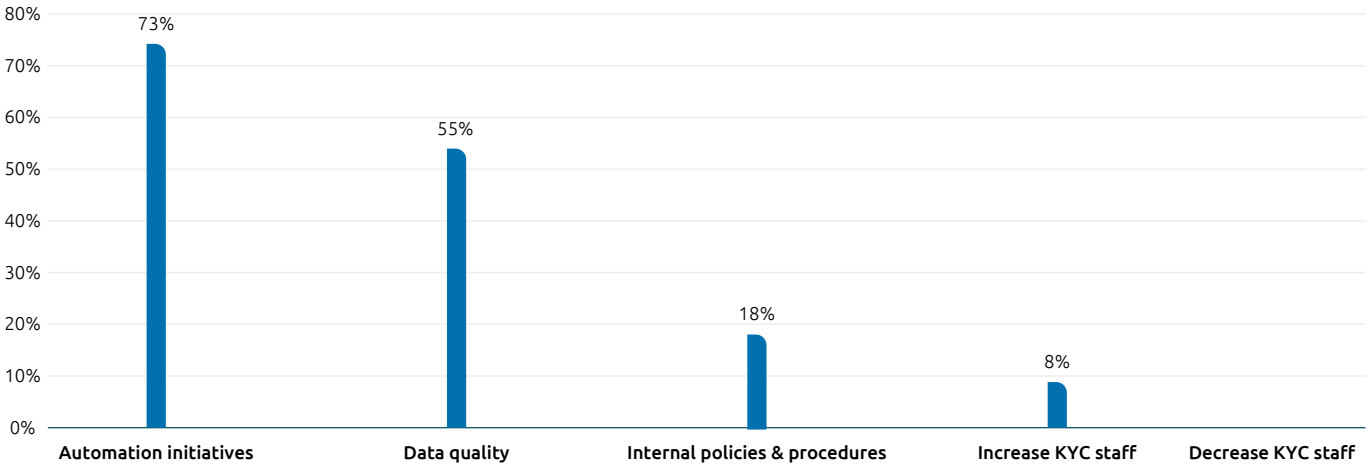
More than half of survey's financial institutions are facing customer complaints with respect to KYC not fostering customer experience

According to our results, over 60% of the financial institutions face customer complaints regarding the KYC process. The most prominent complaint is about the KYC requirements, which is included in 70% of complaints, whereas inconvenience is the second biggest complaint being raised in over 50% of complaints.

Manual workload is the biggest pain point within KYC processes

Internally, the strongest desire is to drive further automation (73%) and improve data quality (55%). The high potential in reducing manual work and duration of KYC processes by lean methodology and automation drives this need. Better data quality allows financial institutions to improve their risk rating and identify risks early. There is almost no intention to either increase or decrease staff, and this might be driven by a tight employee market. A change in policies and procedures is not widely considered, even though it has great potential to decrease the duration of processes.

Figure: 4 **If you could choose freely, what would you improve in your current KYC structure?**



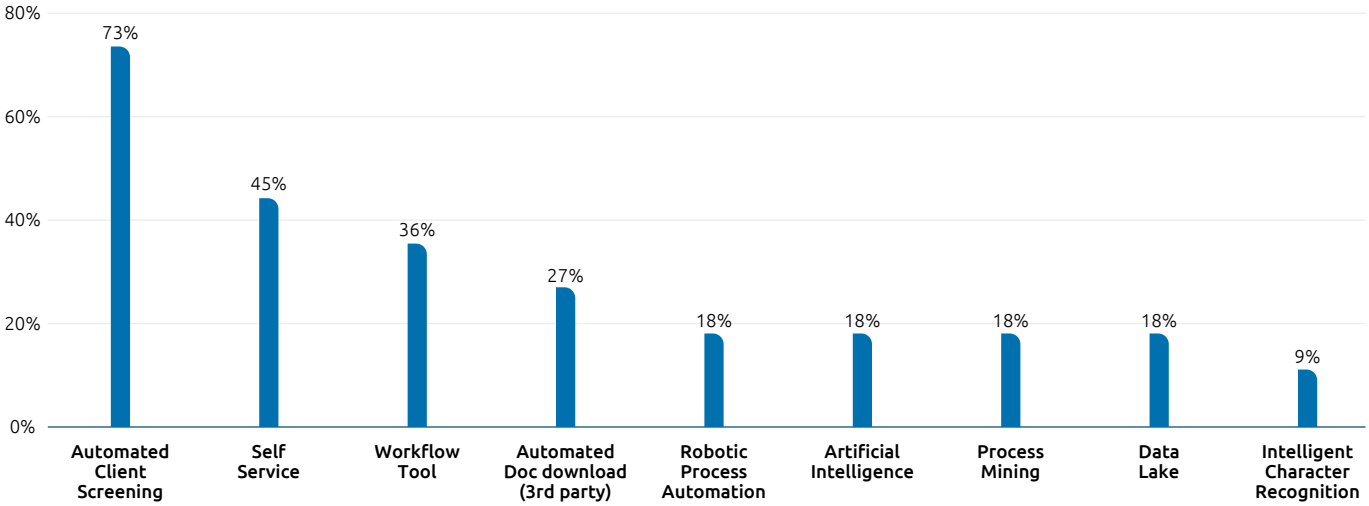
*Multiple answers possible

Another point underlining the desire to increase automation is that banks already using AI (18%) need fewer FTEs in the compliance department.

The potential of technology is not even close to being exhausted, with the use of the main 'technology' being limited to automated client screening

The most commonly used technology by banks is automated client screening (ACS). In over 70% of the banks, ACS is in place as it allows quick detection of sanctioned entities, negative news, or connections to politically exposed persons (PEP). In addition, 45% of the banks already have self-service portals for clients to upload their documents. This option allows financial institutions to gather data directly from the client instead of manually searching and adding data to the client's profile.

Figure: 5 Which of the following technologies are currently already applied in the KYC process in your bank



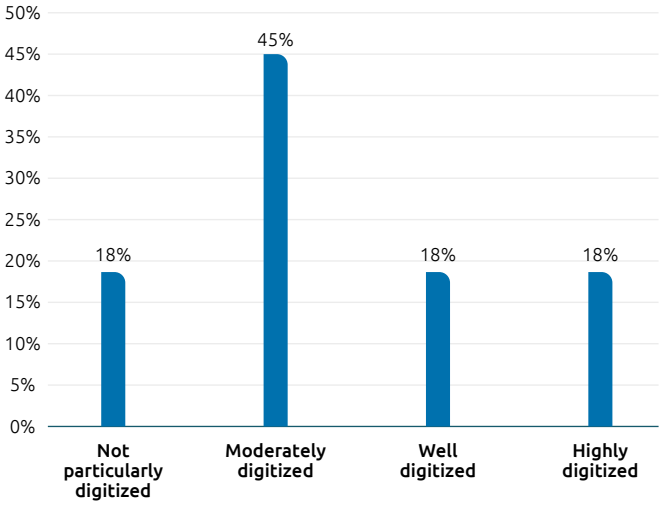
*Multiple answers possible

We analyzed the quantitative data and put that in correlation to our qualitative findings on IT implementation. In our results, we found a negative correlation between having a KYC workflow tool and the duration of an NCA process. This means financial institutes with a KYC workflow tool in place, required less time for their NCA processes.

Technologies are still at the early stage of unfolding their potential within the KYC departments of large banks

Moreover, we identified a large gap between 'self-awareness' of digitization and actual digitization: 63% describe the digitization state as moderately or well digitized, but only 18% currently use robotic process automation (RPA), AI, process mining, or a data lake in the context of KYC.

Figure: 6 What is the digitisation state of your KYC process?



APPENDIX 2: AML DETAILED RESULTS

The banking industry still suffers from high transaction monitoring false positive ratios – on an average 92%

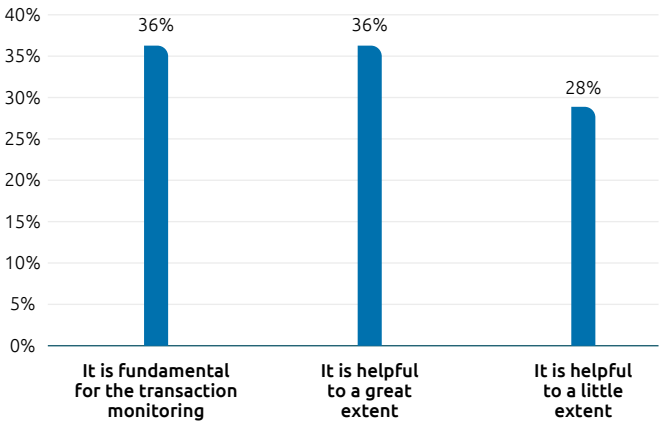
One of the biggest plagues in AML transaction monitoring is the high false-positives ratio. Our study confirms that the banking industry still suffers from high false positives ratios in transaction monitoring – on an average, 92%, with some financial institutions reporting FP ratios up to virtually 100%.

Against our expectation, we could not detect a correlation between the perceived state of digitization of the AML process and the false positives ratio of transaction monitoring alerts: we observed false positives ratio of 97% against perceived digitization ranging from 'not particularly digitized' to 'highly digitized.' Similarly, we cannot confirm a causal relationship between the current usage of advanced technologies such as AI or RPA, and the false-positives ratio.

The degree of tool customization does not have a determining influence on the false positives ratio of transaction monitoring alerts

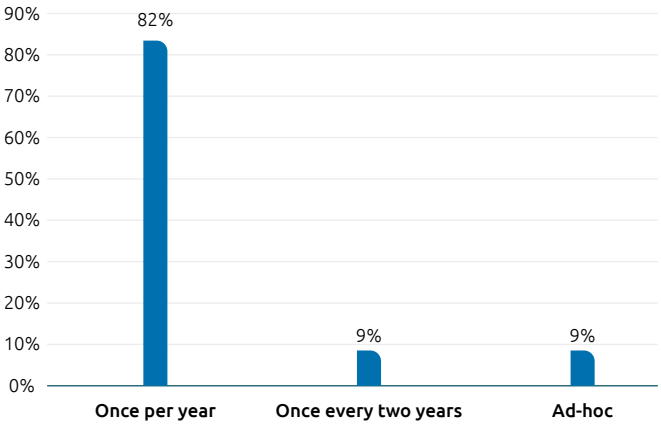
Surprisingly, no correlation can be observed between the degree of AML tool customization and the false positives ratio of TM alerts. While the majority of banks regard tool customization helpful to a great extent or even fundamental with regards to AML process efficiency, the degree of tool customization does not seem to exhibit a determining influence on the false-positive ratio of TM alerts.

Figure: 7 Influence of AML tool customization on efficiency of the AML process



Similarly, the regularity of performing tuning exercises does not seem to affect the false-positive ratio in a causal manner for the participating banks. Most of the respondent banks perform tuning once a year.

Figure: 8 Regularity of tuning exercises



The proportion of suspicious activity reports based on transaction monitoring alerts is very heterogenous among the participating banks

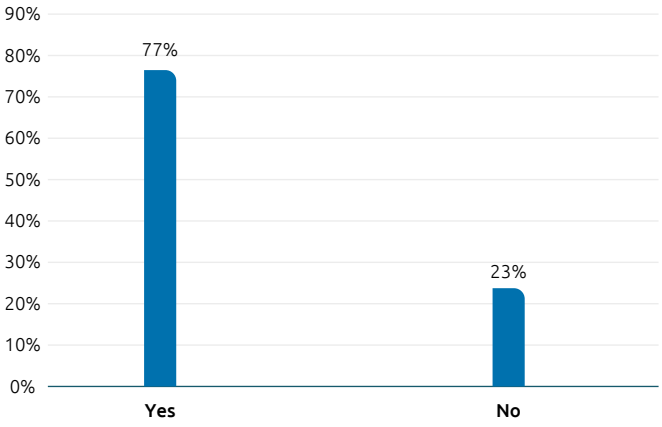
Despite comparable false positive ratios, the participating banks substantially differ in the exhibited behavior with regards to Suspicious Activity Report (SAR) filing. Interestingly, the proportion of SARs based on TM alerts is very heterogenous among the participating banks: quotients from 5% to nearly 100% are observed. This could be traced back to differences in the implemented controls: some banks rely predominantly on automated transaction monitoring screening for detection of suspicious behavior, while others also implement account activity reviews, and reviews of the nature and purpose of the business relationship, which are regularly carried out in the first line of defense. Furthermore, banks of comparable size, in terms of client volumes and distribution between retail and corporate clients in Germany and Italy, differ substantially with regards to filed SARs: German banks file almost 50% more SARs than their peers in Italy. This could either indicate an unlikely scenario of higher risk exposure among the clientele of German banks or more plausibly, a substantially lower risk appetite in Germany. The SARs are filed and sent to the financial intelligence units (FIU), with some of them resulting in non-deviating behavior/false positives.

Vast majority of banks regard their AML process as cost-efficient despite high false positives ratio

The high false positive rates for transaction monitoring alerts clearly differ from the respondent banks' perception of their AML cost-efficiency. The results of our study suggests that an astounding 77% of the banks perceive their AML process as cost-efficient.

Understandingly, participating banks were reluctant to share their overall annual AML costs, despite the anonymous nature of the study. Still, the answers we received paint an interesting picture: universal and commercial banks have similar AML costs/client of approx. EUR 4/client p.a. Investment banks have much higher AML costs/client reaching up to EUR 300/client p.a. The difference is also intuitive as clients of investment banks are much more complex and profitable compared to retail clients.

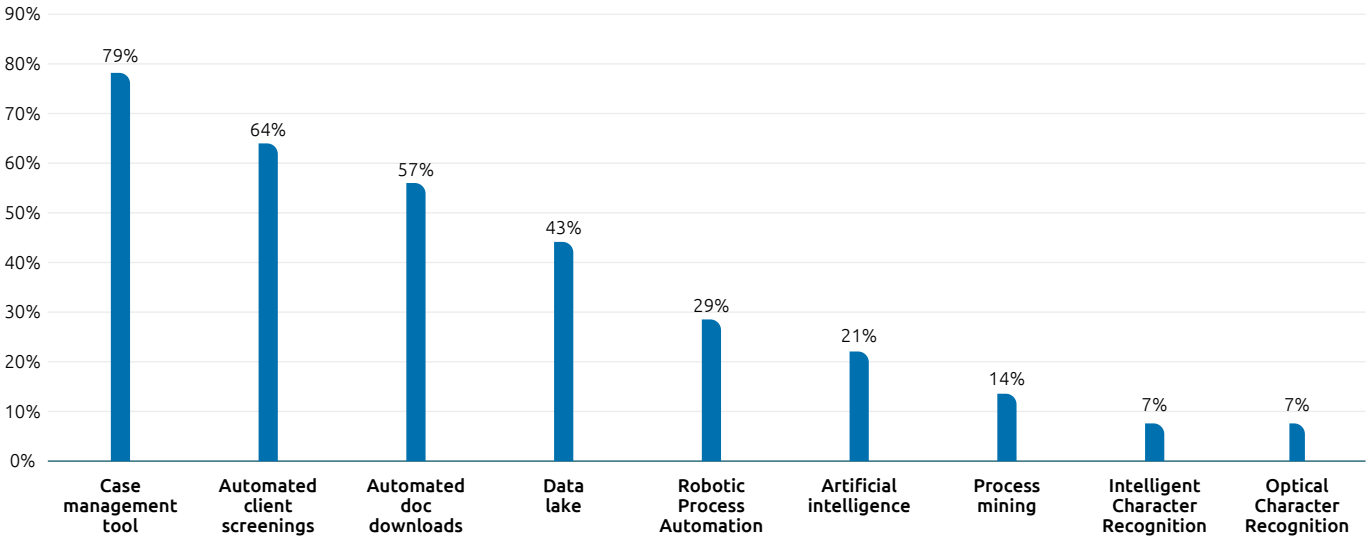
Figure: 9 **Would you consider your Bank as cost-efficient regarding AML?**



The potential of AI & smart automation is currently largely untapped but expected to be at the forefront of technology investments in the next two years

One potential reason for the still overwhelmingly high false-positive rates could be the largely unexplored potential of artificial intelligence and smart automation. While the majority of the respondents perform automated client screenings, employ workflow tools, and make use of consolidated data from third party providers such as commercial registers or databases, only less than half unleash the potential of their in-house data through a data lake. Even more so, less than a quarter of the respondents are currently leveraging artificial intelligence (AI) within their AML processes. Potential reasoning could be the difficulty of justifying AI usage to the regulator as it is sometimes regarded as a 'black box' type of technology. However, substantial steps have been taken in the direction of 'explainable AI,' which has the potential to meet the regulatory requirements towards justification of the algorithms' decision making.

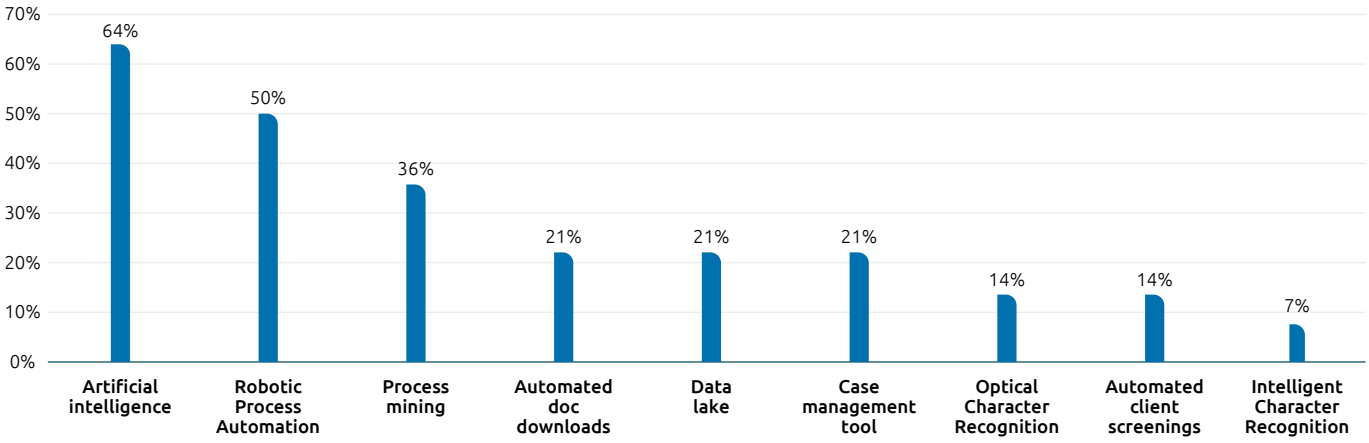
Figure: 10 Current technology adoption within AML process



The General Data Protection Regulation (GDPR) already describes "the right to obtain an explanation of the decision reached" by algorithms, and the EU has identified explainability as a key factor in increasing trust in AI in its white paper and AI-regulation proposal.

As per our study results, it seems; however, that substantial wind of change is blowing in the direction of AI in terms of future investor sentiment. Almost 65% of the respondents are planning on investing in AI in the upcoming 24 months; half are intending to leverage RPA, and more than a third are thinking about exploring the possibilities that process mining offers.

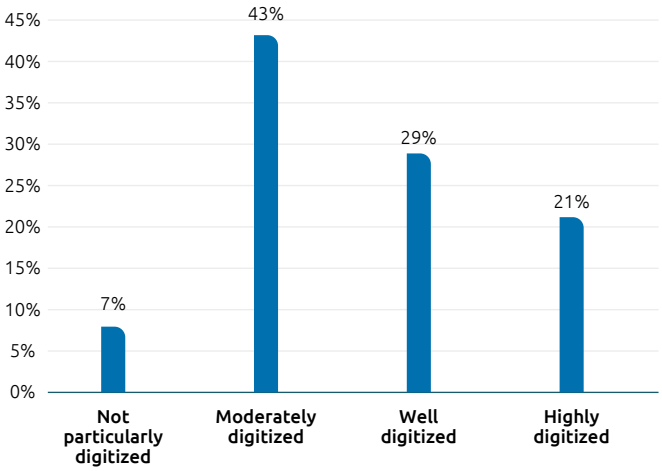
Figure: 11 Potential technology investment areas in the next 24 months



In total, 50% of respondent banks regard themselves as only moderately digitized or not particularly digitized

These results seem largely consistent with the perceived digitalization state of the AML process, as 40% of the respondents regard themselves as moderately digitized and, cumulatively, another 50% as well or highly digitized. There is still potential to improve the digitalization state of the AML process flow by eliminating manual data entry through the usage of optical character recognition (OCR)/intelligent character recognition (ICR).

Figure: 12 Perceived digitalization state of the AML process

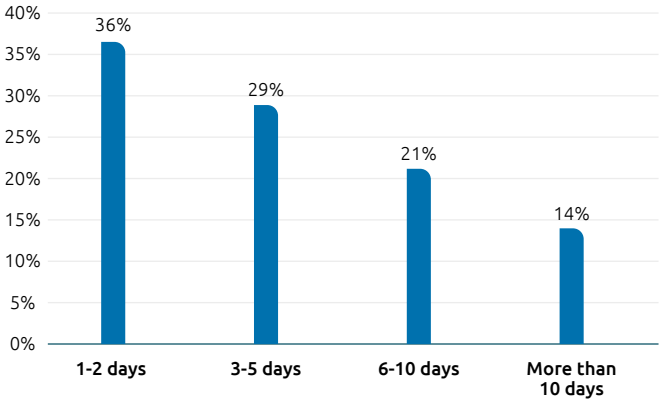


With regards to AML software, the majority of the respondents rely on licensed third-party software (77%), while AML operations remain in-house. Only a quarter of the respondents are currently considering carving out their AML operations and outsourcing them to off-shore/near-shore locations. Two likely reasons are potentially behind this: data sharing restrictions, especially outside of the EU, and/or the major wave of outsourcing to EU wage arbitrage countries having reached its prime.

Only 14% of banks schedule more than 10 days of training for their AML employees

By and large, Anti-Money Laundering employees receive up to 5 days of training per year (65%). Only 14% of banks schedule more than 10 days of training. Given the rapidly evolving regulation, simplification possibilities unfolding through the usage of AI, and unstable situation in Europe and its repercussion for Sanctions, the question arises whether banks should consider increasing the amount of AML training they offer their employees.

Figure: 13 Training days p.a. for AML staff



Interestingly, the ratio between the number of clients and the number of employees is pretty similar among the participating banks (~0.4%) with some minor deviations that have their explanation in the nature of the business model, i.e., purely digital bank or investment bank.

When asked about their plans for efficiency programs and/or staff reductions over the next three years, respondents are unanimous in their answers: continuous incremental improvements to the software currently in use are planned, as are further efforts to standardize processes in all departments, but more and more are envisioning investing in machine learning or other efficiency levers such as model optimizations. While staff reduction per se is not planned, organizations hope to reduce the need for repetitive manual intervention with low added value through the usage of AI and RPA.

04. SUMMARY

Where next for AML?

What are the key trends in the area of AML and how will they impact banks?

AML & increased supervisory scrutiny

In July 2021, the European Commission proposed a plan for a European Authority for Anti-Money Laundering (AMLA) and Countering the Financing of Terrorism (CFT). The AMLA will be established in 2023 and operational by 2024 with authority to supervise anti-money-laundering measures and impose fines across the EU. The focus of the new authority will be on large lenders who operate in at least seven EU member states and are deemed 'high-risk' by at least four.

One major contribution of AMLA will be the creation of a single EU rule book for AML/CFT. The rule book will be based on regulatory standards and harmonized supervision.

Moreover, best practices from member states will be reflected by detailing out rules on customer due diligence' and beneficial ownership.

While the intention of the AMLA is to introduce a consistent framework to ease compliance for obliged entities who are subject to AML rules, especially for those who carry out cross-border activities, it is also expected to be associated with some overall implementation and understanding challenges. Additionally, increased regulatory scrutiny can be expected through the introduction of a new regulatory body.

New behaviors & new money laundering scenarios

As client behaviour changes in the digital age, additionally propelled by the pandemic, so does the behaviour of financial criminals.

The rise of virtual currencies, especially in Eastern Europe and parts of the Middle East, provide a fertile ground for money launderers, who can slip into the financial system more easily and remain hidden.

As transaction monitoring regulations are tight, financial criminals may consider shifting their illegal activities to less regulated areas such as cryptocurrencies and digital currencies.

Despite the introduction of new regulations such as MiCA (Markets in Crypto Assets regulation), which only applies to Europe and does not cover the full scope of crypto assets, there are still loopholes in the money laundering space.

These new placement possibilities are largely not yet reflected in traditional rules-based AML systems, which are already overstrained with complex scenarios.

Therefore, it becomes ever so important to leverage the possibilities of AI, smart automation, and predictive analytics to enable effective and efficient AML screening based not only on historical behaviour, but also on pre-analysed patterns and anomaly detection.

Greater transparency for ultimate business ownership

Recent AML regulation has been steadily shifting focus towards greater transparency concerning ultimate beneficial ownership (UBO). The true ownership of a new corporate client is often buried beneath many layers of complex structures and a constellation of cross-border legal entity types. This makes the identification of the business ownership inherently complex and results in a process that often lasts several weeks. Shareholder information tends to consist of unstructured data, often hidden in paper filings, with no consistency in how it's collected, recorded, or stored. This often means that compliance professionals need to sieve through inconsistently designed forms and partially hand-written documents.

Most of these challenges can be alleviated through the use of AI to simplify UBO search and discovery. For instance, unstructured data from shareholder filings can be turned into machine readable text through the application of optical character recognition. As the next step, this information can be tagged and run through a machine learning-based analysis engine. The final output comprises a structured data set with cross-border shareholder information, visualizing connections between companies, directors, officers, and shareholders.

External Data providers including governmental agencies offering opportunities to collect UBO information centrally. Given intelligent data mapping capabilities, financial institution can reduce the research time by an automated data enrichment.

AML professionals currently find themselves at the intersection of increasing regulation, with the accounting officer bound by the demand for more transparency and a rapidly changing post-pandemic, conflict-fueled world. In this situation, it becomes ever so important to leverage the possibilities provided by data and automation to deliver a better protected AML bank environment and drive down unnecessary costs.

List of abbreviations

FI	Financial Institution
ACS	Automatic Client Screening
AI	Artificial Intelligence
AML	Anti-Money Laundering
AMLA	Authority for Anti-Money Laundering
CFT	Countering Financing of Terrorism
EU	European Union
FIU	Financial Intelligence Unit
FP	False Positives
FTE	Fully Taxable Equivalent
GDPR	General Data Protection Regulation
ICR	Intelligent Character Recognition
KPI	Key Performance Indicator
KYC	Know-Your-Customer
NCA	New Client Adoption
OCR	Optical Character Recognition
PEP	Politically Exposed Person
RPA	Robotic Process Automation
SAR	Suspicious Activity Report
TM	Transaction Monitoring
UBO	Ultimate Beneficial Owner

About Capgemini Invent

As the digital innovation, design and transformation brand of the Capgemini Group, Capgemini Invent enables CxOs to envision and shape the future of their businesses. Located in nearly 40 studios and more than 60 offices around the world, it comprises a 10,000+ strong team of strategists, data scientists, product and experience designers, brand experts and technologists who develop new digital services, products, experiences and business models for sustainable growth.

Capgemini Invent is an integral part of Capgemini, a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 350,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering, and platforms. The Group reported in 2021 global revenues of €18 billion.

Get the Future You Want | www.capgemini.com/invent