NICE
ACTIMIZE

AI in AML: The Shift is Underway

NICE Actimize Insights Report

Ted Sausen
AML Subject Matter Expert | NICE Actimize

As a means to provide trends and changes within the AML landscape in 2020 and beyond, NICE Actimize conducts annual industry surveys to gain a better understanding of the perception variances for Machine Learning (ML) and automation technologies with Anti-Money Laundering (AML) programs.

In this industry survey based on that research, NICE Actimize evaluates the ongoing challenges faced within solutions for transaction monitoring and examines the considerable shifting viewpoints financial services organizations (FSOs) have toward the modernization of AML programs with ML and automation technologies.

The most obvious inferences derived from the survey results show how the sophistication and diversity of today's financial crimes contribute to the complexity of AML solutions and add to the never-ending challenges to maintain an effective AML program. Risk and compliance officers are routinely struggling to find resources to stay on top of their workloads, the volumes of suspicious transactional alerts continue to rise, and regulatory expectations continue to intensify, further contributing to their troubles.

> The global respondents were from a diverse set of FSOs in terms of asset-size, ranging from Tier 1 banks, mid-size banks, and banks with assets under $10 billion. Most respondents had roles in either the risk and compliance, operations, or technology division, with a primary focus area on transaction monitoring.

Some key findings to note before we begin:

- In 2019, about half of respondents indicated alert volumes and alert quality are the most significant challenge within their transaction monitoring solution. This was closely followed by data integrity issues, and the overall cost of compliance.
- Also in 2019, 90 percent of respondents indicated their systems should be tuned between one and four times per year. (More frequent tuning yields reduced alert volumes and their associated costs.)
  - While this is an industry best practice, only half of those organizations responded as being able to perform this as they don't have the available resources (i.e. investigators, technology, other knowledgeable staff).
- Ensuring proper alignment of customer segments is becoming a recognized necessity, as a "one-size fits all" model has not been proving to work.
  - Like tuning, the frequency of segmentation maintenance is not always done as regularly as it should be.
- The sentiment around AI, ML and automation technologies is progressively shifting. As industry use cases have begun to reveal benefits such as reduced false-positives and better quality of alerts, there are plenty of FSOs re-evaluating their existing solutions.
  - Ninety percent of respondents in 2019 indicated they're currently in the process of conducting these evaluations.
- Making do with what they already have is no longer sustainable for FSOs. Staff, resources and the budget to support them are not at the trajectory of the workload, and in many cases are going in the opposite direction. Now that we've entered 2020, this reality is shaping what's to come of AML programs as we progress through this new decade.

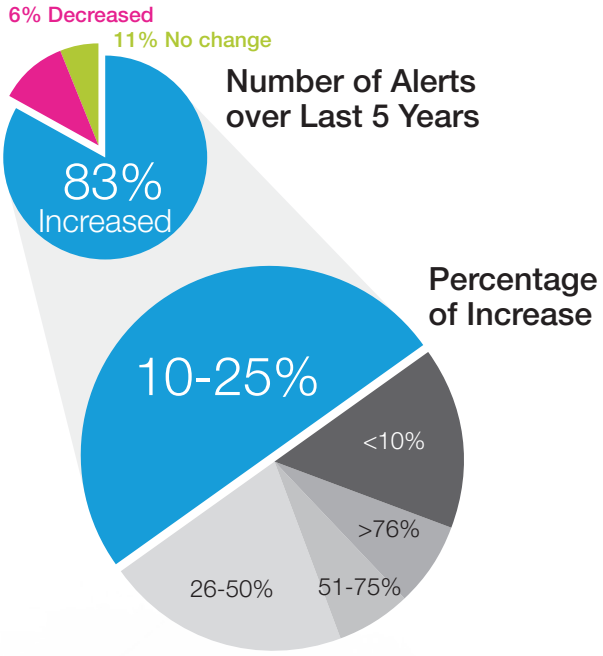
Compounding Transaction Monitoring Workloads

New evolving and dynamic threats combined with stronger governance programs have resulted in a need for new analytics to be added to existing AML solutions to address scenarios such as virtual currencies, human trafficking or terrorist financing. This was confirmed in our latest 2019 study, where half of respondents indicated they're adding these new analytics to their transaction monitoring programs on an annual basis.

New analytics are essential to protecting the FSO; however, their introduction adversely impacts their already demanding workloads. In 2019, 83 percent of respondents saw an increase in alert volumes over the last five years. Most also indicated they saw a 10-25 percent increase in the number of alerts, with some seeing increases as high as 75 percent.

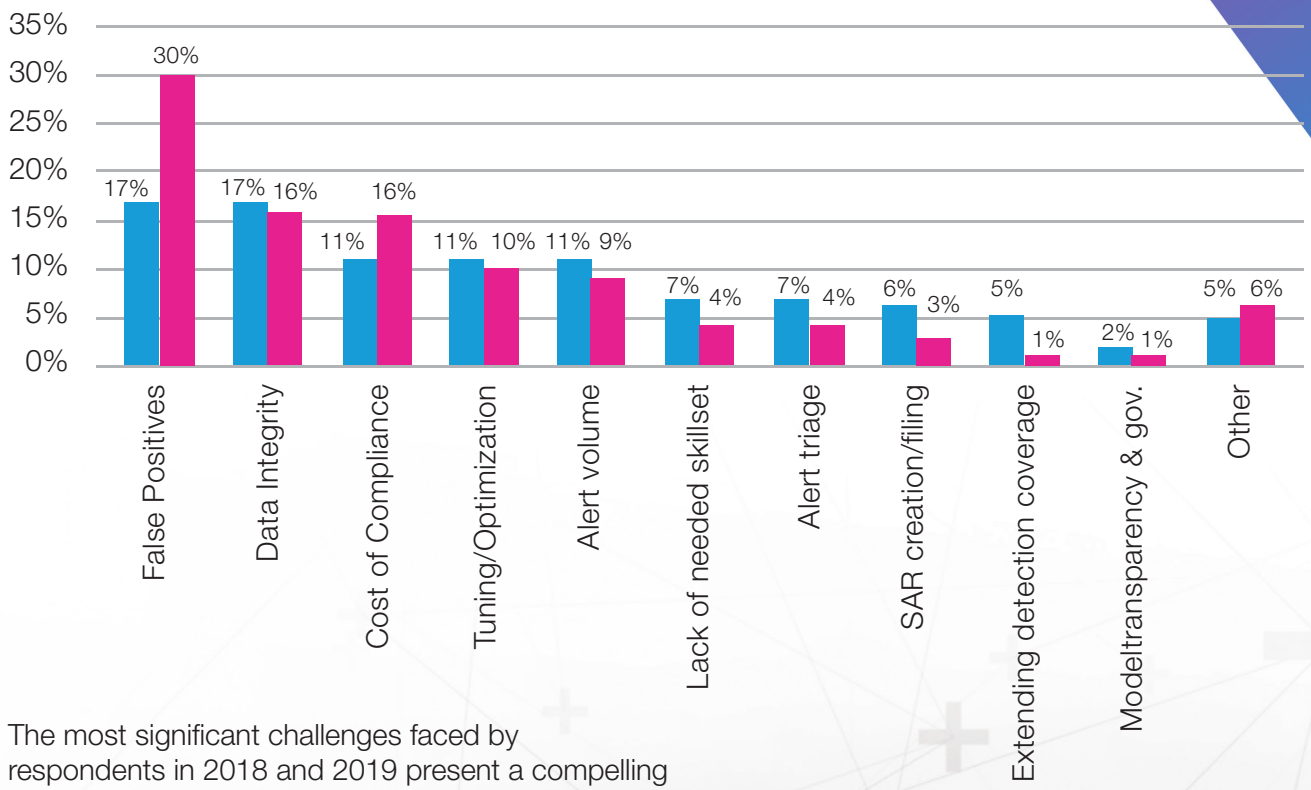
Most alerts in today's transaction monitoring systems are made up of false positives. As there are varying opinions on the definition of a "false positive", for the purpose of this report, we define it as any alert that doesn't result in a suspicious activity report being filed.

False-positive alerts were named the most significant challenge FSOs are currently facing. Results showed almost 95 percent of alerts are resulting in false positives, with some FSOs indicating even higher percentages. It's also important to note, from 2018 to 2019, the number of people reporting this as their most significant challenge had almost doubled.



Dealing with this challenge requires significant efforts on behalf of investigators. To put this into perspective - a major UK-based multinational organization employing around 60,000 AML investigators and compliance officers, stated they typically spend between five and 30 minutes investigating just one low-level false positive.[1] More complex alerts have the potential to take them hours and even days to resolve. This puts a strain on analysts, investigators and compliance staff, and sometimes account managers and other respective roles who may need to step in and help.

Which aspect of your transaction monitoring program is the MOST SIGNIFICANT challenge to your department today?



The most significant challenges faced by respondents in 2018 and 2019 present a compelling observation. The chart above shows an increase in false positives and a decrease in tasks like SAR creation, alert triage, detection, and model validation. **This implies there's a growing maturity in organizations from an operational perspective, and while they have the right people and processes in place, they're still unable to reduce the erroneous alerts that contribute to the overall increasing costs of their AML programs.**

Reworking Technology

Addressing the Problem

Addressing high false-positive rates is a two-step process. First, FSOs need to verify their client populations are grouped appropriately. Ensuring proper maintenance of customer segments is a necessity, as a "one-size fits all" model has proven not to work. Take an example of two gas stations – one may operate as a gas station and convenience store with a commercial ATM, while the other operates as a gas station and convenience store with a private ATM and gaming machines for gambling. Although they're very alike, they should be placed in different segments to be monitored accordingly.

Grouping client populations appropriately allows for a comparison of transactional behaviors between customers with similar characteristics. When certain activities fall outside the typical behavior of these segments, an alert is then generated. In practice, review of these segments should take place on an annual basis. If possible, more frequent reviews are beneficial as customers can move to a different segment if necessary, based on their behavior. It's also important to keep in mind that behavior can change from the time the customers are onboarded, through the course of their relationship with the organization. Improper maintenance of segments will misclassify activities as being unusual, therefore triggering additional alerts. What it really comes down to is creating highly-targeted segments with common attributes based on behavior and risk. Having very similar peers helps to meticulously optimize thresholds.

Segmentation Management

Between the 2018 and 2019 surveys, there was great similarity in responses to the management of segmentation. Most organizations surveyed review their segmentation at least annually, with 75 percent stating they've reviewed them within the last two years. Considering the initial lack of attention paid to segmentation in the past, this shows the industry taking a positive step forward.

The second step in addressing high false-positive rates is tuning analytical models. Tuning is the process of optimizing the parameters and thresholds to ensure they're appropriate for each of the defined segments mentioned previously. The biggest challenge is how the effort is multiplied exponentially when more segments are created. FSOs must determine the appropriate number of segments to effectively monitor their customers, without creating a scenario where the effort of tuning is exorbitant, preventing it from being performed on a regular basis. We stress the importance of proper segmentation because without it, appropriate parameters cannot be set for clients with dissimilar activities.

Ninety percent of respondents in 2019 agreed tuning should be done at least once per year, as more frequent tuning yields reduced alert volumes and their associated costs.

While this is industry best practice, only half of those organizations had the available resources to perform tuning (i.e. investigators, technology, other knowledgeable staff). Many organizations have chosen to tune a subset of their model instead, but this means they never have a fully tuned model.

Due to the number of variables involved, it's becoming humanly impossible to achieve these activities effectively when using traditional methods. This is why FSOs are beginning to pivot from traditional methods and explore approaches incorporating machine learning and clustering techniques.

90%

agree tuning should be done at least once a year

AI and Machine Learning: The New Norm

The introduction of machine learning and AI to the AML space was initially faced with varying degrees of reluctance. Analysts, investigators and regulators were accustomed to traditional rules-based models they could understand, whereas machine learning comes with a different approach. The inputs and the outputs of the models are known, but the processes that take place in between are not as transparent or understandable.

In 2018, justifying models enhanced by machine learning to regulators was the number one concern for compliance teams, with the second concern being the costs to implement them. Interestingly, just one year later in 2019, there was a swap – making implementation costs the number one concern and putting justification to regulators second. Based on these results and other industry observations, regulatory acceptance is no longer such a big concern. FSOs have gone from "cautiously observing" to actively pursuing these technologies to complement their existing AML programs.

The changing sentiment has been prompted by a culmination of a few factors:

- The results started becoming real. Early adopters who had kickstarted their experimentation were observing positive results.
- Select vendors were quick to respond to the lack of transparency of "the black box" and developed explainable analytics to relieve any apprehension.
- Backing and encouragement by regulators.

The removal of regulatory barriers resulted in a few takeaways:

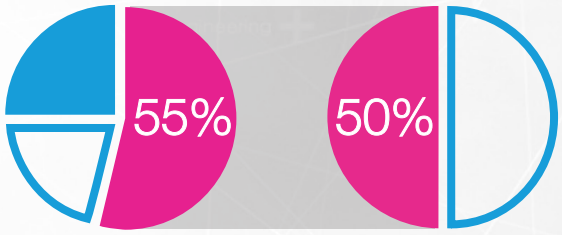
- FSOs would be granted a safe harbor and wouldn't be punished or penalized should these innovative technologies uncover new money laundering schemes not previously detected by their conventional AML programs. This alleviated uneasiness of organizations thinking they'd need to perform costly look-back exercises.
- Regulators will not penalize organizations who choose not to implement new innovative technologies – which prompts the question: "Why even mention this?".

In 2019, 15 percent of respondents stated they still do not believe machine learning would easily comply with regulations. Responses to a further series of questions uncovered they do in fact believe these new technologies, but their confidence wanes when the time comes to finding data scientists to implement them. These suspicions are typically due to the costs required to integrate, their aversion to risk, and their lack of a plan accurately mapping out the ROI.

15%

Do not believe machine learning would easily comply with regulations

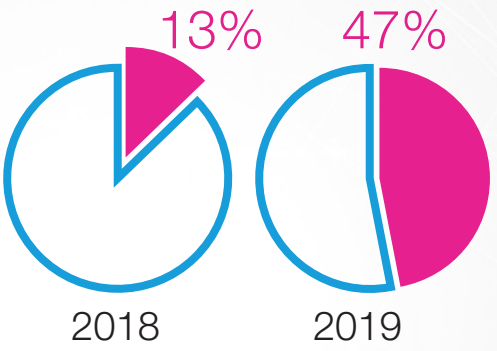
On the flip side, 25 percent of respondents had already integrated AI and machine learning technologies into their existing AML solutions, with over half of respondents stating they're actively evaluating. Of that number, 50 percent then specified they intend to integrate them within the next year.



25% Have already implemented AI
55% Currently evaluating
20% Not evaluating or planning

Out of 55% evaluating, half are intending to integrate within next year

In both 2018 and 2019 surveys, respondents expressed their main business drivers for machine learning in AML as anomaly detection, segmentation and model tuning (both of which are used in tandem). **We found it particularly interesting that "machine learning for segmentation" as a business driver had made a notable jump from 2018 to 2019 – with an increase from 13 percent to 47 percent.**



Machine learning for segmentation

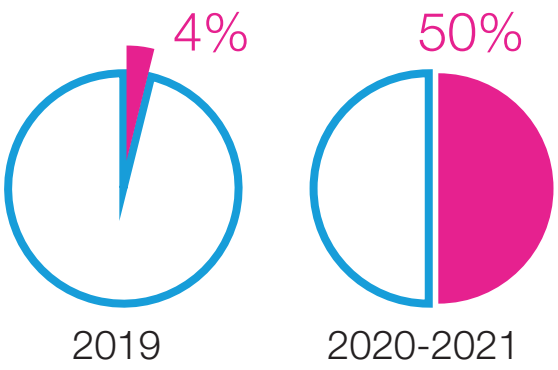
With most organizations trending toward AI, machine learning and automation technologies, the days where they'll be the new norm, and perhaps even a requirement, are swiftly approaching.

Leaning into Cloud

Effectively implementing machine learning within AML programs means relying heavily on large amounts of data, which brings a host of requirements and demands. To make this manageable, many FSOs are turning to the cloud. The top two drivers for cloud indicated by respondents were ease of integration with other technologies and the scalability it offers. Additional benefits of a cloud-based solution include:

- Reduced costs (cloud-based storage and other hardware)
- Better options for computing performance with increased agility
- Data science resources (such as those offered as a service by third-party providers)
- Collective intelligence from data leveraged across multiple organizations (peer benchmarking and advanced anomaly detection)

With only four percent of respondents in 2019 stating they're currently using public cloud-based AML software and services, a sweeping 50 percent are planning to use public cloud within the next two years.



Moving Forward

Looking ahead in 2020 and beyond, the industry will prioritize the modernization of AML programs at a rapid pace. Case studies exhibiting the quantifiable benefits of new technologies have begun to surface and organizations who have yet to embrace the shift will use them as validation when building their own business cases to justify the spend.

Thus far, much of the focus from a machine learning and AI perspective has been around transaction monitoring, but we'll start to see this expand into processes for screening and customer due diligence. Machine learning will leverage large amounts of client attributes combined with transactional activities to further identify anomalies in behavior, as well as reduce much of the "noise" existing in so many transaction monitoring systems today.

It's important to understand how weaknesses in the KYC process will degrade the entire KYC/CDD program, having a downstream effect that impacts other areas such as transaction monitoring and watch list filtering. Using the latest technological innovations allows for an expanded risk reach and simplifies all aspects of the entire customer lifecycle assessment – accounting for KYC application onboarding, ongoing CDD and enhanced due diligence processes, for an integrated AML solution. This results in operational efficiencies and provides a holistic view of customer risk so FSOs can rest assured their understanding of their customers is always up-to-date.

2020 will be a year of action for all the financial crime technology themes that dominated 2019, as well as the few years prior. There are five key areas expected to emerge from these themes and dramatically impact financial crime fighting and anti-money laundering activities as we move forward:

1. Private-to-private information sharing
2. Increasing adoption of contextualized financial crime
3. Real-time AML monitoring
4. Quality not quantity impacts
5. Greater alignment of standards

One thing is for certain – financial crimes will continually evolve and become increasingly complex. This is a war your organization needs to win. NICE Actimize is here to help and always ready to take a deeper plunge into the topics and approaches we've covered in this study. Feel free to reach out to us and stay tuned for further insights into latest developments and outlooks for the AML industry.

Citations

1. McGowan, J. (2018). AI Made to Reduce False Positives. Celent, 3–3.

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.