AMLYZE

AML Readiness report 2023

Introduction

Dear Report Reader,

AML/CFT is a critical element for any financial institution, fintech, neobank and any other obliged entities.

It is therefore particularly important not only to remain aware of the compliance rules and regulations which may trigger adjustment of your internal controls but also to properly understand the most common mistakes and how to avoid them.

The main purpose of this report is to raise awareness of challenges compliance teams deal with on a daily basis and to encourage discussion on whether they are being dealt with properly.

Because after all, AML/CFT is the one area where there's no room for compromise and where mistakes can have critical consequences for your institution and its reputation.

We wish you an interesting and valuable time while reading and we as AMLYZE would be happy to contribute to the success of your Anti-Financial Crime compliance processes.

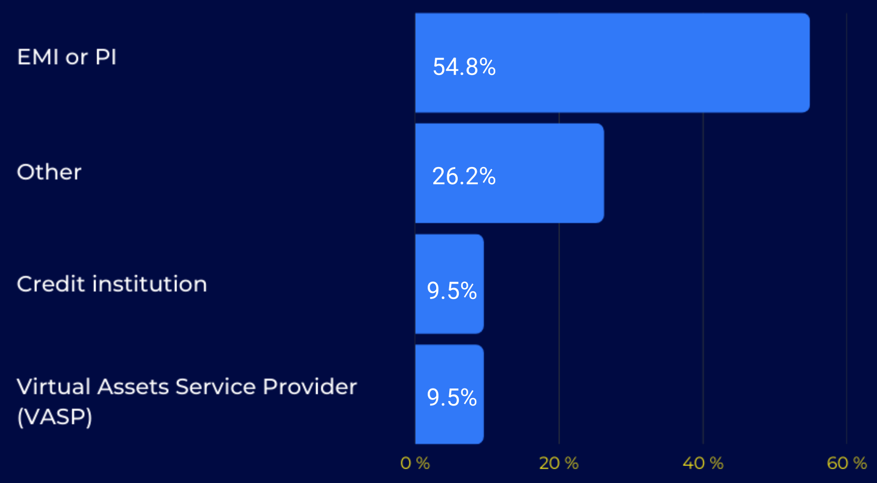
The AMLYZE team

Basic facts about the survey

- → Submissions of the survey: 52
- → Respondents who completed the survey: 42
- → Number of questions asked: 24
- → Average time spent to complete the survey: 6 min 32 sec
- → Demographics: 37 from Lithuania, 2 from Latvia, and 1 from Cyprus, Finland, Moldova
- → Type of survey: anonymous
- → Date: Dec. 2022 - Feb. 2023

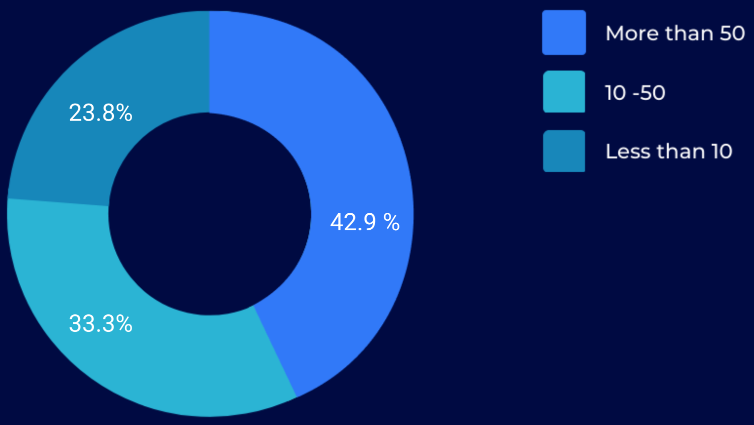
1. What type of license does your company have?

More than half of our respondents (55%) are licensed but we also have a fair share of Virtual Assets Service Providers (VASPs) and Credit Institutions (10% each).



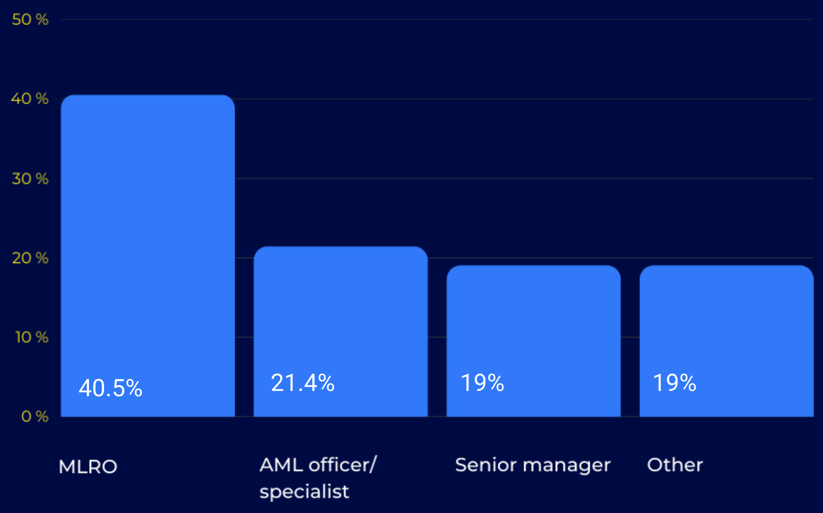
2. How many employees does your company have?

Most of the respondents (43%) are from medium size (>50 employees) organizations, which is not surprising in the view of the previous result.



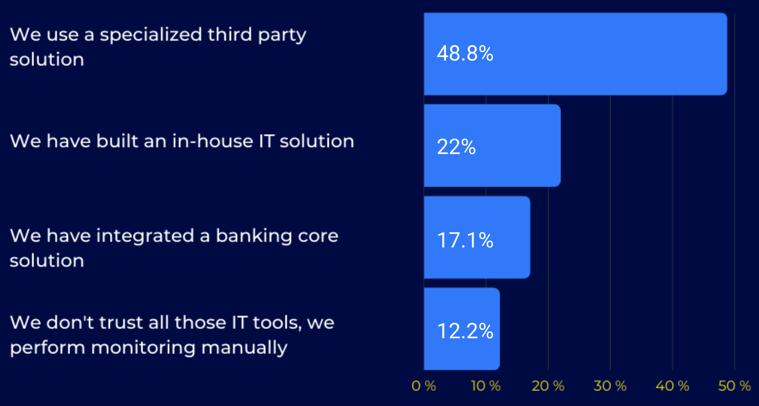
3. What is your position within your company?

The majority of respondents are compliance professionals with senior (MLRO) or mid senior roles (AML Officer/Specialist) within their organizations.



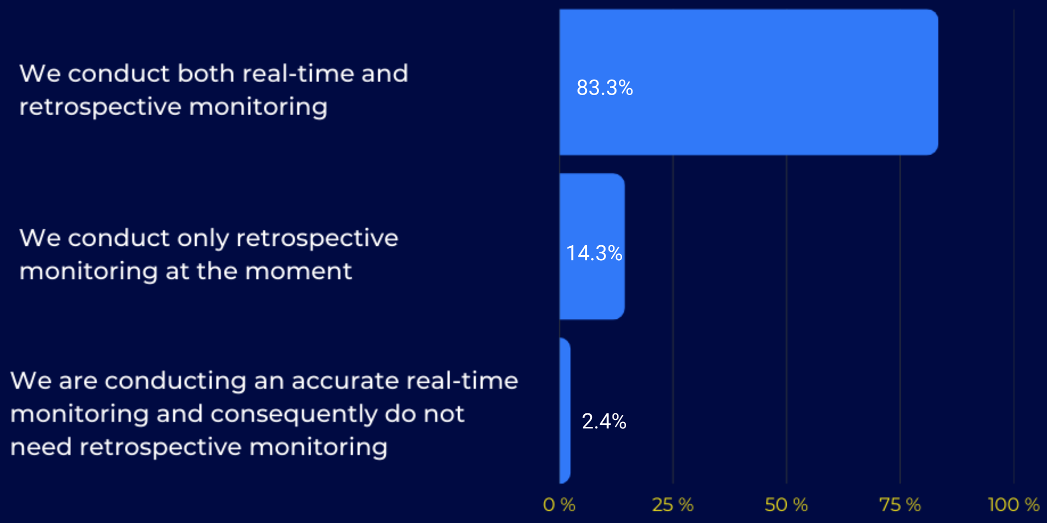
4. Do you use a specialized IT tool for transaction monitoring purposes?

It is interesting to see that, although the majority of respondents use a specialized third party solution, a significant part (22%) has still made the choice to build a solution internally and more than 15% still perform monitoring manually, possibly because of a low volume of operations.



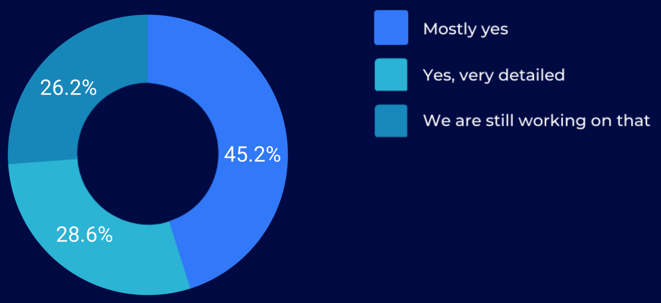
5. Do you or your company's IT tool conduct real-time as well as retrospective monitoring (aside from sanctions screening)?

The vast majority of respondents use both real-time and retrospective monitoring, although just under 15% currently use only retrospective monitoring. The proportion of those who do real-time monitoring only and do not need retrospective monitoring is completely insignificant.



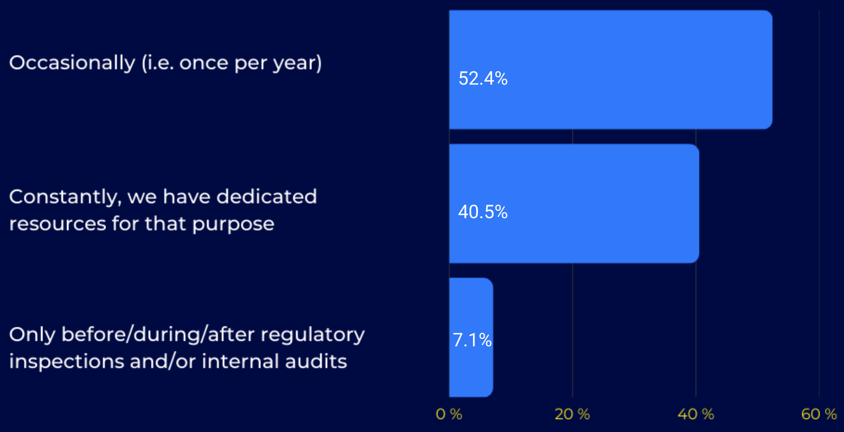
6. Are monitoring rules, solutions and techniques clearly defined in your internal procedures?

More than a quarter of the surveyed organizations have not yet clearly defined their monitoring rules and methodologies as part of their internal procedures. In case of regulatory inspection, this could be seen as a breach of compliance and result in a warning or a fine.



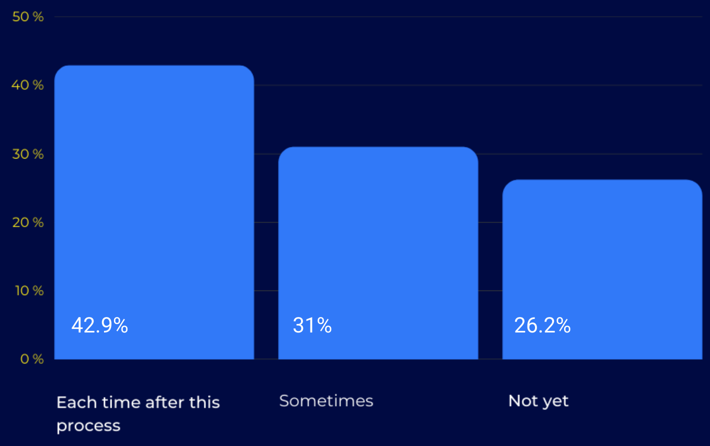
7. How often do you test and update your monitoring solutions/tools?

Monitoring solutions and tools are tested and updated occasionally in more than half of the organizations and constantly in just over 40% of the organizations. However, more than 7% of organizations only do this before or after regulatory inspections (internal audits), which exposes them to a much higher risk of breach, warning or fine.



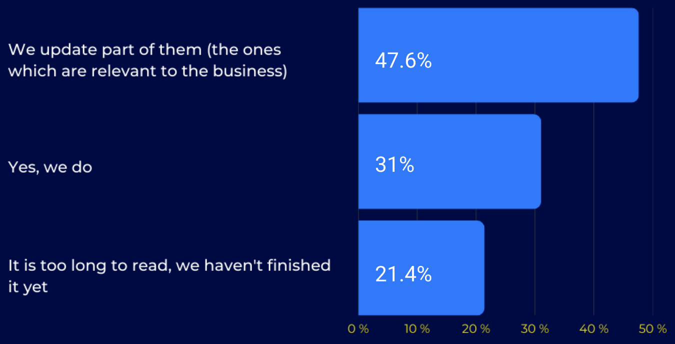
8. Do you update your scenarios library after performing your ML/TF own-risk assessment (EWRA)?

The majority of respondents (43%) do not consistently update their scenario library after conducting their own ML/TF risk assessment which, on top of exposing them to an increased regulatory risk, also means that their current set of monitoring scenarios is not adapted to their actual risks.



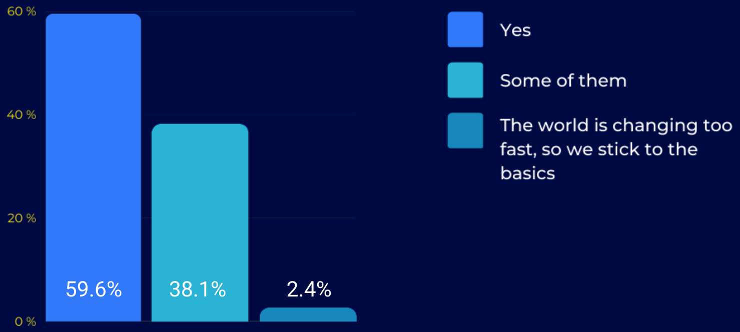
9. Do you update your scenarios library after the Lithuanian national ML/TF risk assessment is published?

As for updating the scenario library after the publication of the Lithuanian national ML/TF risk assessment, a third certainly do so, while slightly less than half update some of them, or at least the ones that are relevant to their business. A fifth say that it is too long to read and they simply can’t finish it, which is likely to result in outdated and/or inadequate transaction monitoring scenarios and increased risk of warning and fines.



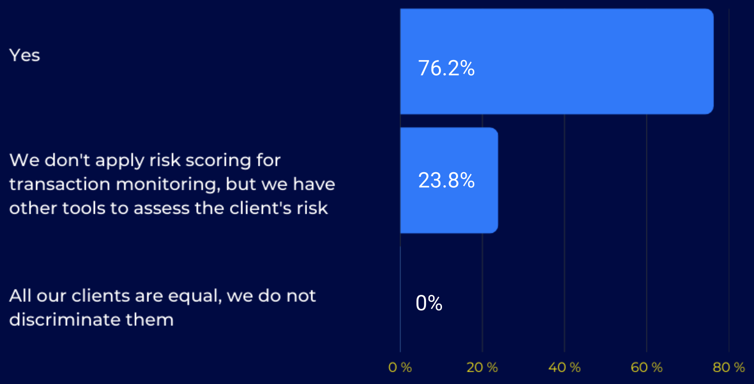
10. Do you take into account emerging global risks, while selecting the most suitable monitoring solutions?

Everyone would probably agree that considering global risks when selecting the most appropriate monitoring solutions should be a good practice, although the survey shows that only 60% do so and even 38% only consider some of the risks. This trend may also be related to the fact that it is challenging for some organizations to assess the full scope of global risk they are exposed to, because they lack resources to perform a thorough EWRA.



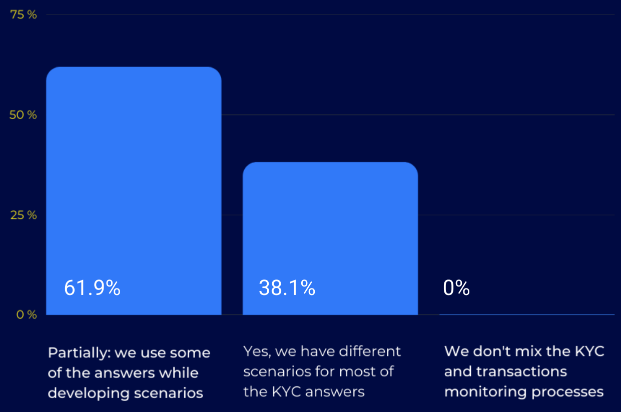
11. Do you consider your client's risk score while monitoring?

Almost a quarter of respondents do not take the customer risk score into account when monitoring, which possibly means that they face high numbers of false positives which could be avoided if they would apply a risk based approach.



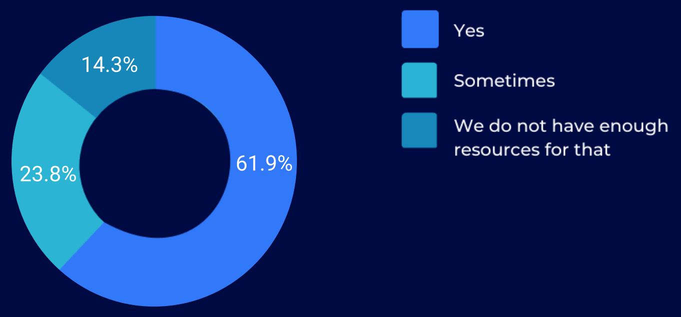
12. Do you consider specific clients' KYC questionnaire answers as part of your clients' transactions monitoring process?

The same way as for the previous answer, more than a half of respondents that only partially use their KYC questionnaire data, could increase their efficiency by adapting their monitoring scenarios to the specificity of their customers profiles, thus avoiding a significant number of false positives.
Considering KYC questionnaire answers for clients' transactions monitoring process is a practice done only by 38% of the respondents while the remaining part does it just partially – they use some of the answers while developing scenarios.



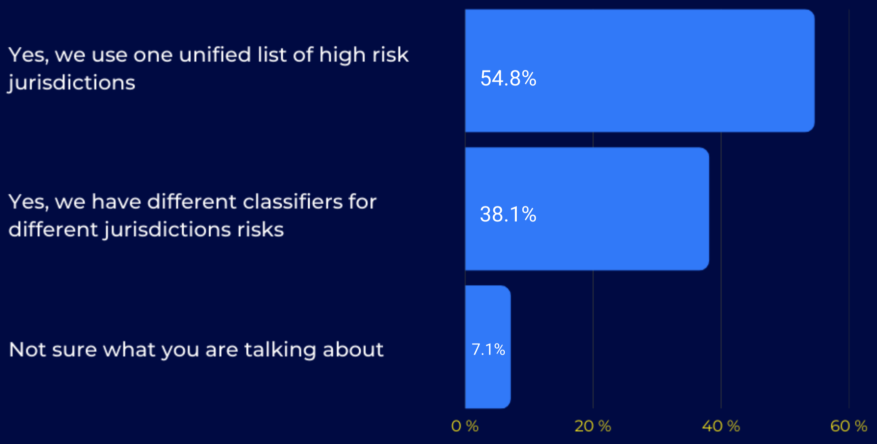
13. Do you classify your clients into specific groups to understand which intensity and scale of monitoring are best suited?

The majority of respondents (62%) categorize clients into specific groups to understand the most appropriate level and intensity of monitoring, although a quarter only do this occasionally and 14% do not have the resources to do so.



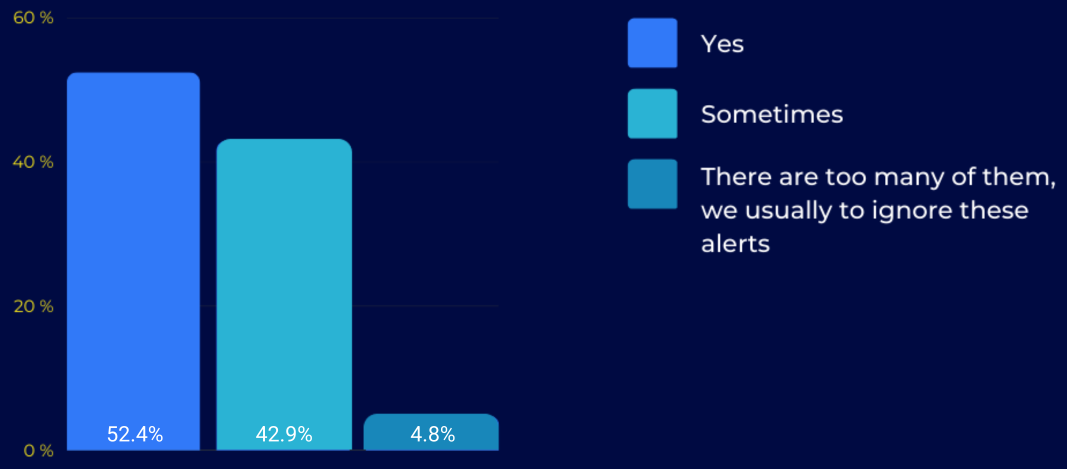
14. Do you have different scenarios for different types of geographical risk?

More than half of respondents use a single list of high-risk jurisdictions for different types of geographical risk, while slightly less than 40% have different classifiers for different jurisdictional risks.



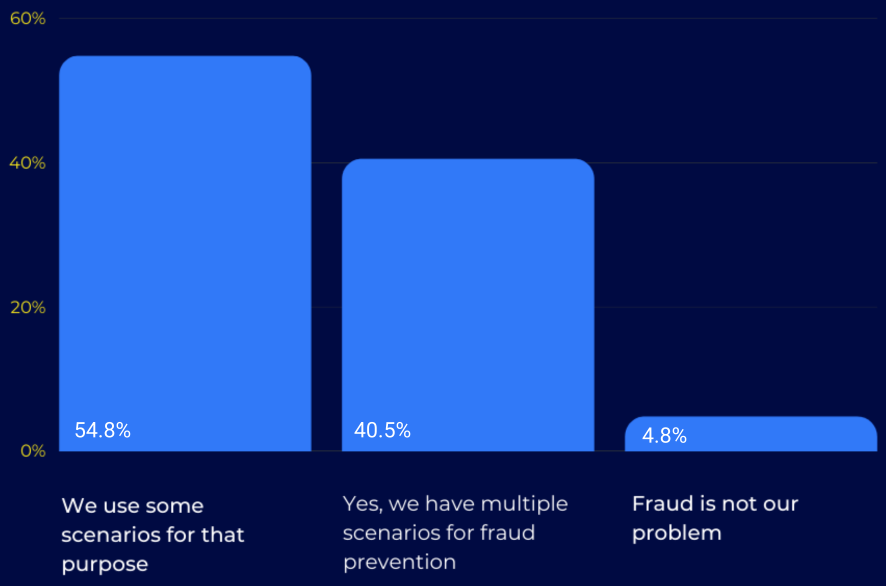
15. Do you measure the ratio of false-positive alerts to evaluate the effectiveness of each scenario?

Measuring the rate of false positives to assess the effectiveness of each scenario should be the way forward for every MLRO, but the reality is that only 43% do this sometimes and 5% even ignore alerts because they seem too frequent.



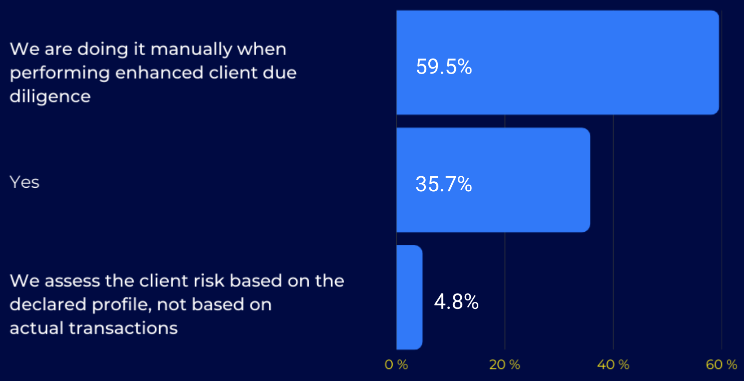
16. Do you use monitoring scenarios, which are aimed at preventing fraud?

Every company subjected to AML should use multiple scenarios to prevent fraud, but only 41% do so, while more than half (55%) use some scenarios for this purpose.



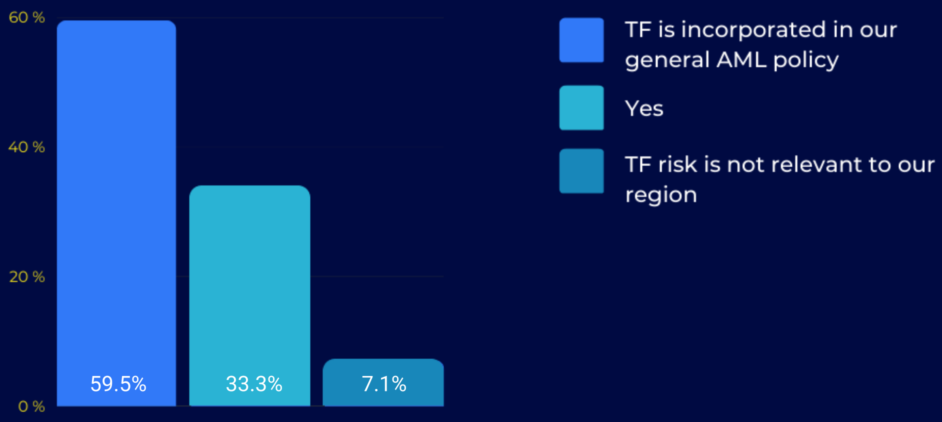
17. Do you re-calculate the clients' risk automatically in case the clients' activity doesn't match with the initially declared profile during the KYC process?

Just over a third of companies automatically recalculate the risk of a customer if the customer's activities don't match the profile originally declared during the KYC process, while 60% do this manually when carrying out enhanced customer due diligence.



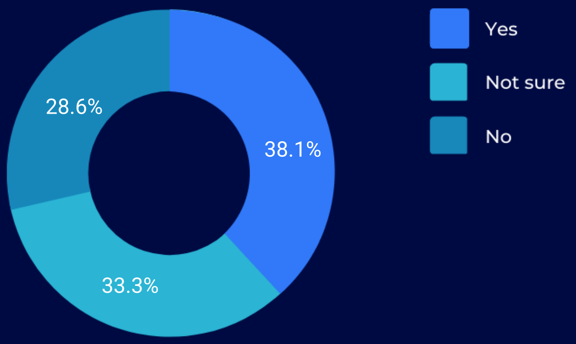
18. Do you have separate procedures and monitoring scenarios to spot potential terrorists financing (TF)?

More than 90% of companies identify potential terrorist financing either directly or as part of their general AML policy, although 7% of respondents say that TF risk is not relevant to our region.



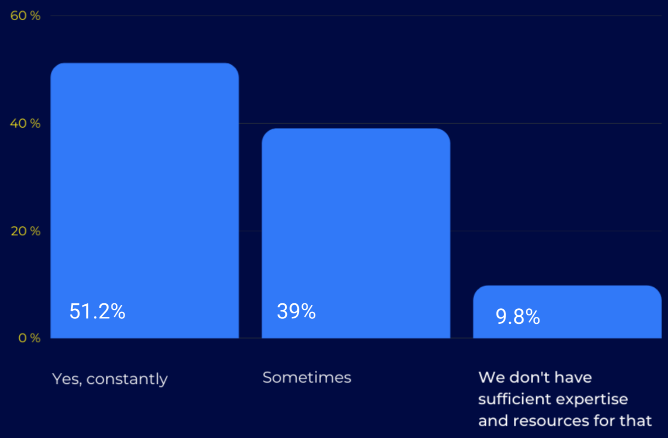
19. Do your monitoring scenarios consider logs with IP addresses from terrorism financing high risk countries?

A third of companies are not sure whether they consider logs with IP addresses from high-risk countries for terrorist financing in their monitoring scenarios, and just under 40% do so. This practice is not used at all by 29% of companies.



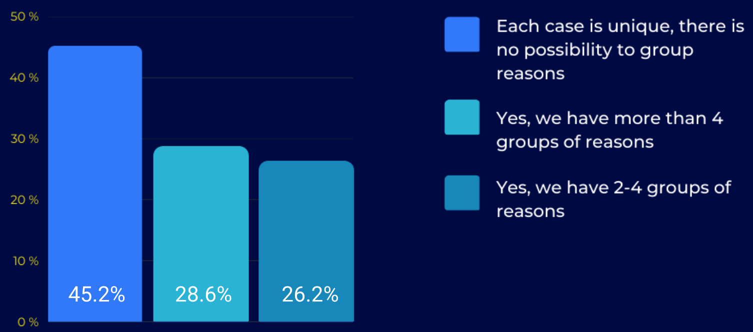
20. Do you use the outcomes of internal investigations for the transactions monitoring scenarios development?

39% of companies only sometimes use the results of internal investigations for transaction monitoring and 10% don't use them at all due to a lack of resources and expertise. Only 51% of companies use them all the time.



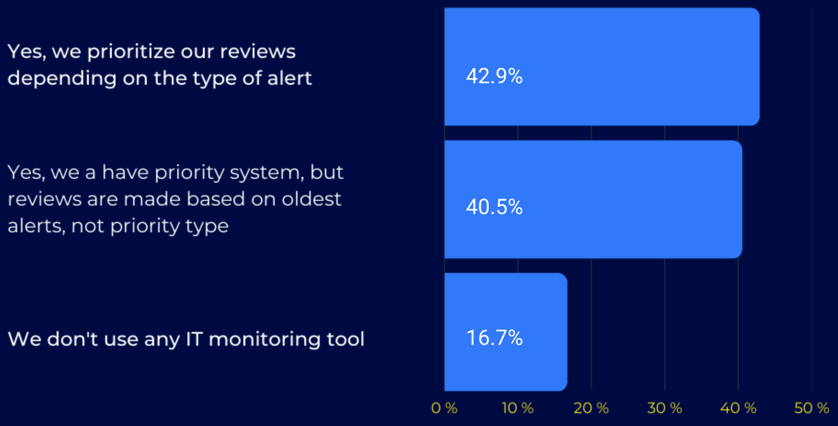
21. Do you have internal investigations outcomes classifiers (or groups) enabling you to provide reasons for the final decision (as well as for statistics and analytics purposes)?

The regulator recommends that the results of internal investigations should have as many classifiers (or groups) as possible to provide reasons for the final decision, and the survey showed that only 29% of companies have more than 4 groups of reasons. Just over a quarter of companies have 2-4 groups. Most of the companies (45%) say that there is no possibility for them to group reasons because each case is unique.



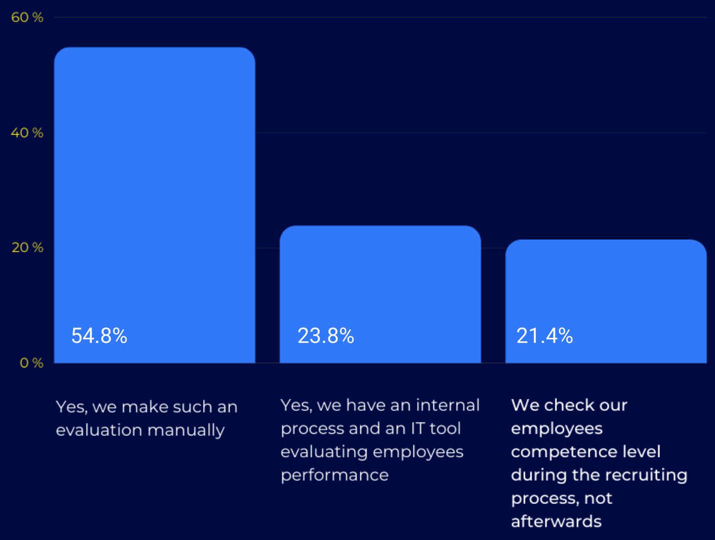
22. Have you set a priority system on alerts in your IT monitoring tool?

Prioritizing alerts in the IT monitoring tool should be the way to go, although only 43% of companies do this and 41% have a priority system, but reviews there are based on the oldest alerts, not the type of priority. 17% of companies don't use an IT monitoring tool at all.



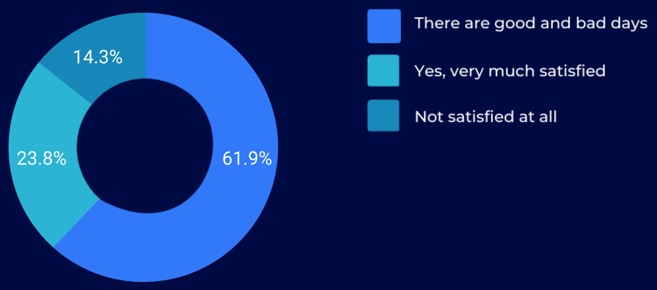
23. Do you periodically assess the work quality of each individual employee working on monitoring?

More than three quarters of the companies surveyed could gain in efficiency by automating the assessment of their team member work's quality and by making it periodically.



24. Are you satisfied with your transaction monitoring tools and systems?

Only less than a quarter of companies are very satisfied with their transaction monitoring systems and the majority (62%) of respondents say that there are good days and bad days. Meanwhile, 14% of companies are not at all satisfied with the system they have in place.



Main survey outcomes

- Transaction monitoring solutions and tools are tested and updated occasionally in more than half of the financial institutions and 7% of these organizations only do this before or after regulatory inspections (internal audits)
- The majority of companies (43%) do not consistently update their scenario library after conducting their own ML/TF risk assessment which, on top of exposing them to an increased regulatory risk, also means that their current set of monitoring scenarios is not adapted to their actual risks
- 43% of organizations only sometimes measure the rate of false positives to assess the effectiveness of each scenario although this should be the way forward for every MLRO, and 5% even ignore alerts because they seem too frequent
- Only 41% of companies subjected to AML are using multiple scenarios to prevent fraud, while more than half (55%) use some scenarios for this purpose
- Just over a third of companies automatically recalculate the risk of a customer if the customer's activities don't match the profile originally declared during the KYC process, while 60% do this manually when carrying out enhanced customer due diligence
- Only 51% of companies constantly use the results of internal investigations for transaction monitoring, 39% do that sometimes and 10% don't use them at all
- Only less than a quarter of companies are very satisfied with their transaction monitoring systems

Key conclusions to consider

Survey conclusion I. Enterprise-wide risk assessment is a self-standing exercise and does not affect monitoring scenarios and rules.
Risk (!) The transaction monitoring scenario library is not targeted to the inherent risks the institution is exposed.

Survey conclusion II. Testing process is not part of the continuous transaction monitoring cycle.
Risk (!) The existing monitoring tools are not effective and not efficient due to: data input problems, inappropriate data conversion, improper model calibration, number of false positives leading to non-productive investigations and increasing workload.

Survey conclusion III. Introduction of the transaction monitoring process into the overall AML/CFT risk management process has certain shortcomings (1): the customer‘s behavioral pattern either does not affect his/her risk score or the risk score is not being changed in due time.
Risk (!) The existing monitoring scenarios based on the client‘s risk score might be ineffective due to the poor data quality.

Survey conclusion IV. Introduction of the transaction monitoring process into the overall AML/CFT risk management process has certain shortcomings (2): internal investigations are not being used as the internal source of information to better understand certain typologies.
Risk (!) The monitoring scenarios are not aligned with the certain behavioral patterns, trends and even possible ML/TF typologies that are relevant for the company.

Would you like to discuss your company's AML/compliance situation in person?

We are open to that!
Just drop us a message to info@amlyze.com and we will get back to you!