Guidance for maintaining effective and efficient Sanctions Screening Systems

27 February 2025

ΕΠΙΤΡΟΠΗ ΚΕΦΑΛΑΙΑΓΟΡΑΣ ΚΥΠΡΟΥ
CYPRUS SECURITIES AND EXCHANGE COMMISSION

TABLE OF CONTENTS

Introduction

During the period April-November 2024, the Cyprus Securities and Exchange Commission ('CySEC') conducted **thematic inspections to assess the effectiveness and efficiency of the Sanctions screening systems used by a sample of regulated entities**. All types of regulated entities (Cyprus Investment Firms 'CIFs', Administrative Service Providers 'ASPs', Funds and Fund Managers, Crypto Asset Service Providers 'CASPs') were subject to these thematic inspections. CySEC's inspections focused on the legal requirements emanating from the provisions of the United Nations Security Council Resolutions or Decisions (UN Sanctions) and the European Union Council's Decisions and Regulations (EU Restrictive Measures), specifically for screening the UN and EU Sanctions Lists to identify designated persons, as well as screening practices for U.S. and UK Sanctions Lists. All regulated entities must ensure that they have in place adequate internal policies, procedures and controls, in accordance with the nature and size of their business activities and customers.

The **scope** of the thematic inspections was to test the client and transaction screening tools used by regulated entities and to assess their effectiveness and efficiency. For these purposes, effectiveness means the ability of the screening tool to create a match against the name of a designated person, while efficiency means the number of alerts/hits generated by the screening tool per name screened. During this process, different automated screening systems (both in-house and third-party provided) were tested, as well as manual practices.

Testing included **Control tests** (sanctioned names as they appear on Sanctions lists sources and are not adjusted) and **Manipulated tests** (sanctioned names that have been adjusted using an algorithmic manipulation e.g. misspelled names, wrong dates, words duplication, missed words, etc). The testing process considered the following key questions:

1. Does the screening tool generate an alert when an exact or 'unmanipulated' sanctioned name is screened? (Control test)

2. Are the 'fuzzy matching'[1] rules, configuration and threshold settings effective, such that the screening tool generates an alert when a 'manipulated' sanctioned name is screened? (Manipulated test)
3. Is the level of 'false positives' generated by the screening tool manageable?
4. Is the screening tool performance in line with its 'peers' (industry comparison), global standards and CySEC's expectations?

CySEC appointed a third-party company, which specialises in testing the effectiveness and efficiency of screening systems, to assist in conducting these thematic inspections. This expert firm supported CYSEC in conducting the testing, providing analysis, benchmarking the results and providing feedback on the test results.

The **purpose** of publishing these guidelines to all regulated entities is to share the outcomes and feedback of these thematic inspections, clarify CySEC's expectations on screening practices and provide guidance on best practices in testing, tuning and optimisation of screening systems for overall sanctions screening compliance.

[1] Fuzzy matching is a technique used to identify similar elements in a particular data set. It is traditionally used for name matching when undertaking customer screening and identifies approximate matches rather than exact matches.

Weaknesses/Deficiencies identified

The most important **weaknesses/deficiencies** identified during the thematic inspections are:

- **Limited understanding and knowledge of the functions and capabilities of third-parties' screening tools used** ('out-of-the-box solutions'). Some regulated entities were not aware that their screening system's configuration settings (e.g. screening parameters and thresholds) could be adjusted/calibrated, either internally or by their vendors at their request. This had a detrimental impact on the effectiveness and efficiency of their screening system's performance.
- An overall **underperformance on most tested metrics versus global standards**, particularly in respect of:
  - **Ability to identify manipulated names**, i.e. names that are similar to names on relevant sanctions lists ('fuzzy matching'), for example spelling errors, omission of characters, words swapping, etc.
  - **High number of returns/hits** (possible matches that need to be manually investigated by the regulated entity to assess whether the matches are 'false positives'). The occurrence of a high number of matches when screening a name (false positives), must be within manageable levels i.e. can be thoroughly investigated without overburdening the associated compliance staff.
- A high number of regulated entities have **manual screening processes** in place. This is causing concerns related to **ongoing screening** of customers (refer also to Circular C318 on automated screening systems). It is very difficult to manually screen against all important Sanctions Lists for all business relationships (not only for actual customers but also their counterparties), when there are additions or amendments on these Sanctions Lists, especially nowadays where sanctions are imposed on a higher frequency. Manual screening may be feasible for a small number of customers, but contains the risk of human error. **Regulated entities with manual screening processes in place should assess the possibility of switching to automation or establish a policy on when they will switch**

to an automated screening tool e.g. when number of customers/transactions increased to a certain threshold.

- A high number of regulated entities were not able to **test their screening system on an automated (batch) basis**, which is essential for quality assurance.
- A limited number of regulated entities have **effective and efficient testing and auditing programs** in place.
- **Ongoing screening practices** vary greatly amongst regulated entities that underwent these inspections.
- **Over-reliance on third parties/vendors for screening purposes** was evident. Also, over-reliance on groups policies and/or other regulated entities own screening processes.

Poor Practices

The most important **poor practices** identified during the thematic inspections are:

- In one instance, a regulated entity **has not tested and tuned with appropriate configuration settings a new screening system before implementation**. After the results of the thematic inspection for the particular screening tool, it was evident that its efficiency and effectiveness levels were very poor and well below global standards.
- In one instance, a regulated entity's screening tool **did not generate expected alerts against sanctioned names as they appear on Sanctions lists**. After examining the situation, it was evident that the version of the screening tool used during the testing process had not been updated to the current version. After updating the screening tool, the issue was addressed.
- In one instance, a regulated entity, due to its **complete reliance on a third-party vendor for sanctions screening**, failed to complete CySEC's thematic inspection.
- In several cases, where regulated entities were using two or more screening tools, the **effectiveness of the screening tools used within the same regulated entity was different** (i.e. one screening tool was producing an alert for a sanctioned name, but the other screening tool used was not), meaning that the configuration settings of the screening tools were not calibrated in the same way, thus producing different results.
- In several cases, the screening tools used **were not producing alerts for names classified as 'weak aliases'[2]**, thus not identifying and matching 'weak aliases' names to sanctioned persons.
- In one instance, a regulated entity, following the results of the thematic inspection for its screening tool, decided to **increase the effectiveness levels of its screening tool to 100%** by calibrating the system parameters of the 'fuzzy matching'. However, the regulated

[2] 'Weak alias' name is a term used for a broad or generic alias name of a sanctioned person or entity, that is included in the official text of the relevant Sanctions List, and could generate a large volume of 'false-positive' hits when such names are screened against.

entity **has not assessed how these changes will affect the efficiency of the screening tool**. As a result, the efficiency levels deteriorated and compliance staff are now facing significantly higher number of hits/alerts per name search and will require more time to investigate alerts in a qualitative manner and clear the false positives alerts.

- In one instance, a regulated entity's screening tool **did not generate the expected alerts against designated persons who are considered deceased, but still appear on Sanctions lists**. After the regulated entity's investigation, it was evident that the exclusion of deceased individuals from sanctions screening was due to a 'Deceased filter' applied in the sanctions screening tool. It is noted that the screening tool used must identify all sanctioned names appearing on Sanctions lists, irrespective of the person being confirmed as deceased or not. The primary reason for keeping deceased designated persons on Sanctions Lists is that their assets should remain frozen and not allowed to be used by their inheritors for unknown purposes. The regulated entity has implemented remedial actions and has deactivated the 'Deceased filter' previously applied in the sanctions screening tool.

Best Practices

The most important **best practices** identified during the thematic inspections are:

- The vast majority of the regulated entities that were using, to some extent, manual systems and controls for screening purposes, have opted to improve their screening capabilities by **switching to automated screening solutions**. Some regulated entities have enhanced their existing screening system by adding further features, such as batch screening, while others have acquired new automated screening solutions.
- Some regulated entities that had opted to change their screening system to a new one, have proceeded to **calibrate, tune and test the settings of the new system, until it was performing to the required standards**, prior to using it for their business.
- Some regulated entities have included in the policies and procedures of their Sanctions Manual, that **testing the performance of their screening tool (e.g. for the appropriate configuration settings) will be done annually**.
- The vast majority of the regulated entities **have subscribed for relevant alerts of Sanctions Lists updates** from important Sanctions Authorities (e.g. EU, UN, US, UK).
- The vast majority of the regulated entities, following the results of the thematic inspection for their screening tools, have proceeded to **optimise their screening system by calibrating its settings**. This was performed by configuring the screening system to take account for 'weak aliases' names, alternative and native spellings, manipulated data, etc. Furthermore, the screening systems were adjusted for dataset sensitivity ('fuzzy-logic') and was calibrated to find the optimum threshold, where effectiveness was achieved at 100% and efficiency standards were met for manipulated data.
- For some regulated entities, after the new settings were implemented on the screening tools used, the average number of alerts/hits, for 'manipulated' data, showed a modest increase compared to the results of the thematic inspection, slightly exceeding global standards. The regulated entities were aware that the adjustments made to the screening tools have deteriorated their efficiency, to some extent. To remedy this, a **robust review**

process was established to ensure that each alert is thoroughly examined and that dedicated persons in the compliance team were made responsible for reviewing alerts. The regulated entities should also continuously monitor the efficiency of their screening tools and the associated workload on the compliance teams.

- The vast majority of the regulated entities, after adjusting their screening system settings to an optimum level in terms of effectiveness and efficiency, as described above, have proceeded **to re-testing their screening system's new settings**. This was performed by repeating the same testing method used during the thematic inspection, namely by sample testing and by using similar datasets, i.e. data from official Sanctions Lists (control dataset) and internally-produced manipulated data (e.g. misspelled names of sanctioned persons), thus comparing the results of the old and new settings. By including 'manipulated' data (e.g. misspelled names, wrong dates, words duplication, missed words, etc.) in the re-testing process, the new settings could be evaluated to assess whether they could account for manipulated datasets.

- Following supporting evidence received from the regulated entities which participated in the thematic inspections, as well as verification by their Internal Auditors of the corrective measures taken, it was evident that the **re-testing performed** for both control and manipulated datasets showed that the adjustments of the screening systems' settings, such as **optimizing name-matching thresholds and refining other system settings (e.g. enable for 'weak aliases' screening), have significantly improved the effectiveness and efficiency of the Sanctions screening systems used**.

- Regarding **manipulated data** (e.g. misspelled names) that might be manually inserted in a screening tool, some regulated entities have communicated to CySEC that their **updated policies and procedures during onboarding is mitigating this risk**. Specifically, when a new customer is onboarded, the customer completes his details to an application form and uploads the requested KYC documents in the regulated entity's system (such as proof of identity and a recent utility bill). The back-office team then reviews this information to ensure that the customer's full name, date of birth, ID/passport number, nationality and documents expiration dates match those on the provided KYC documents. If any discrepancies, such as typos, are identified, the back-office team makes the necessary corrections in the system to ensure consistency with the customer's

information. This ensures that all customer's details, such as name, nationality and date of birth, are an exact match to the official identification documents provided, thereby reconciling the data to be used for screening purposes to ensure data integrity and completeness.

Common reasons for ineffective or inefficient sanctions screening systems

Most screening tools have similar technical abilities and functions. The key to achieving appropriate levels of effectiveness and efficiency is to understand the use and capabilities of each specific screening tool. **CySEC wishes to explicitly emphasize that the configuration and setup of the screening tool is far more important than the selection of the screening tool itself. Improving the efficiency of the screening tool used is critical, as irrelevant results from the screening process can be decreased through careful optimisation of the efficiency of the screening tool used. Time used by compliance staff to assess produced alerts, which are subsequently identified as false-positives, could be more productive if allocated to investigating suspicious transactions.** Normally, when a screening tool is found not be performing as expected, it is due to a combination of the following reasons:

- The screening tool is being used with **inappropriate configuration settings**. For example, if the threshold settings are close to 100%, it will only produce alerts for exact, or near exact, matches of sanctioned records.
- The screening tool is being used with **'out of the box' factory settings, without being tailored to the unique circumstances and risk profile of the regulated entity**. This can occur due to over-reliance on third parties/vendors for screening purposes, where the actual users have a limited understanding of the screening tool's configuration settings.
- **The effectiveness and efficiency of the screening tool is not appropriately balanced. As previously explained, effectiveness means the ability of the screening system to match name searches to sanctioned records (as many as possible relevant hits), while efficiency means the ability of the screening tool to produce as fewer as possible irrelevant hits.** In some cases, screening tools could be very effective in identifying sanctioned records (even manipulated), however, the number of hits produced that are false-positives is high and therefore the system is not deemed to be efficient, resulting to operational risks. Vice-versa, the screening system could be performing very efficiently with few false positives, however, the screening system is ineffective for screening

manipulated records (e.g. misspelled names of sanctioned persons), therefore missing sanctioned records. Both effectiveness and efficiency of the screening systems used are dependable on its configuration settings, i.e. threshold, rules, 'fuzzy logic', etc.

- The **screening tool's current version, operating rules and/or configuration settings have not been updated** in a reasonable timeframe or following significant changes in sanctions regulations.
- The screening tool's **Sanctions Lists are not fully up to date**, due to delays from the vendors. Also, problems with the regulated entity's list feed in keeping up with list providers updates.
- **Poor list management**, too many or not enough sanctions sources are being screened against.
- **Testing of the screening system used has not been performed,** or no clear testing procedures have been set. Most vendors offer a testing environment for their screening tools solutions, where the users can test how the screening tool is performing.
- **Insufficient support from senior management** in the screening processes.

Supervisory Expectations

Sanctions screening are a set of controls that must be embedded within regulated entities' overall controls to detect, prevent and manage sanctions risks. Sanctions screening should form part of an effective Sanctions Compliance Programme, with the purpose to identify possible connections of sanctioned persons and entities with the regulated entities' business relationships, as well as potential sanctions circumvention activity to which regulated entities may be exposed. In January 2019, the Wolfsberg Group published **guidance on Sanctions Screening**[3] to aid financial institutions on assessing the effectiveness of their sanctions screening systems, which contains useful information on how sanctions screening should be deployed. On the same note, the EBA has recently published guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures[4], with focus on the implementation of adequate screening processes.

CySEC expects all regulated entities to consider the findings of the thematic inspections, regarding weaknesses/deficiencies and poor and best practices identified, as described in this Guidance Paper, and assess how their current practices fit against these findings and overall CySEC's expectations. If the regulated entities or their internal auditors identify any weaknesses in their policies, procedures and controls for their sanctions screening systems, it is expected that remediation plans within a specified timeframe should be prepared to correct these weaknesses and ensure compliance with all relevant legal and regulatory obligations.

CySEC also expects that the screening tools used will be regularly reviewed in terms of their effectiveness and efficiency, making sure that they remain relevant to the current business activities and external risk factors.

[3] Wolfsberg Group, January 2019, Wolfsberg Guidance on Sanctions Screening.
[4] EBA, November 2024, Final Report on Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures

The regulated entities can **minimise their risks of non-compliance with relevant regulatory requirements** by, for example:

- **Senior management is committed to promoting sanctions compliance** within the regulated entity. Senior management should have a good understanding of sanctions screening policies, procedures and controls, should receive reporting on a frequent basis in a risk-based manner and actively assess and approve sanctions compliance programs.
- Ensure that **appropriate oversight and responsibilities, as well as accountability in cases of non-compliance** exist regarding sanctions compliance.
- Ensure that adequate **written policies and procedures are in place**, approved by senior management, communicated to relevant personnel, and periodically reviewed to remain appropriate with applicable legislation. Regulated entities should have clear and comprehensive written policies and procedures to demonstrate how sanctions screening obligations are fulfilled.
- Consider the **level of human and technical resources** needed to review alerts in a timely manner. If the number of alerts per name search is considered overburdening for the current level of resources, then the screening tool's configuration and threshold settings should be re-evaluated.
- Ensure that adequate **internal escalation processes** for alerts of sanctioned persons are in place.
- Ensure that all employees have adequate and ongoing **training** on sanctions issues.
- Consider conducting **independent and regular testing to assess the effectiveness and efficiency of the screening tools used,** including before the implementation of a new screening tool acquired. When the testing results are not appropriate, consider tuning the configuration and threshold settings to improve the effectiveness and efficiency of the screening tools used.
- Consider whether the effectiveness and efficiency of the screening tools used **continue to be in line with the regulated entity's current business activities,** external risk factors and supervisory expectations.
- Consider undertaking **periodic reviews** in a risk-based manner of all customers' business relationships and related parties to assess the possibility of connections with sanctioned persons. Periodic reviews could also be triggered when significant events occur, such as

large number of new designations/EU Restrictive Measures or significant increase of customers being onboarded.

- In cases of **group-wide screening** policies, procedures and controls, these should be adapted to meet local regulatory requirements.

Furthermore, the regulated entities can **minimise compliance risks associated with the screening tools used by**, for example:

- **Understand the functions, strengths and weaknesses of the screening tools used**, especially prior to implementation to operations. It is very important to have a proper understanding and adequate skills to operate and manage effectively the screening tool internally, without undue reliance of external providers.
- Assess if the screening methodology used, i.e. **manual versus automated software**, fit the purposes and the needs of the regulated entity.
- The **choice and setup of the screening tool should be dependent to the size, nature and complexity of the business activities and customers relationships** of each regulated entity, as well as its exposure to sanctions risks.
- Ensure that the screening tools used, either internally-generated or provided by third parties/vendors, are sufficiently calibrated, according to the current business activities and external risk factors, and the **configuration and threshold settings are tuned so as to improve their effectiveness and efficiency**. It is very important that the screening tools used do not miss any sanctioned names.
- Conduct **regular testing to assess the level of effectiveness and efficiency** of the screening tool used and find their optimum balance, in accordance with the regulated entity's policies, through calibration of the system settings. **The screening tool should be calibrated so that is working as effective as possible (no sanctioned names are missed), but at the same time is working efficiently i.e. not generating excessive numbers of 'false positives'** that would require disproportionate resources for investigation of these alerts. Although effectiveness of the screening tool is very important in meeting legislative obligations, efficiency should not be disregarded, as low levels of efficiency will stretch the resources needed to assess and clear alerts as 'false positives', thus may result in missing potential true matches due to not investigating all matches. When efficiency is

low, regulated entities should assign adequate resources to manage increased numbers of alerts.

- Understand **which Sanctions Lists the screening tool is screening against and the expected results produced,** especially when these Sanctions Lists change i.e. additions of new designated persons or other amendments. Appropriate Sanctions lists and sanctions regimes programs (e.g. EU Terrorism list) must be selected to screen against, in accordance with legal obligations and internal policies.
- In the cases of screening tools provided by third-party vendors, ensure that **Sanctions Lists changes/amendments are quickly and effectively implemented by the vendors**. Sanctions Lists that the screening tool is screened against, must be up-to-date.
- Monitor the level of alerts/hits per name search, considering 'false positives' numbers, to ensure that **results generated by the screening tool are manageable with current resources and alerts are investigated qualitatively and within the set time limits**. The screening tool, if working efficiently, should not generate excessive numbers of 'false positives' per name search.
- **Document alerts/hits resolution assessments in a structured manner** e.g. information considered, work performed to conclude on 'false positives', users undertaken the work. Alert resolutions should consider variations in names due to translation and spelling.
- **Invest** in automated software and human resources for sanctions screening.
- Use **complete, current and accurate customer information** for sanctions screening.
- Sanctions screening must **account for all relevant data categories,** not only customers' names, but also for **connected parties** of customers (e.g. minority beneficial owners, directors, secretaries, authorized signatories, vendors, customers of the customer, etc.), transactions data (e.g. payer, payee, financial institutions involved, description, etc.) and other relevant data. The relevant data categories that will be screened should be documented accordingly in the internal policies and procedures e.g. Sanctions Manual.

Ongoing Screening Practices

CySEC expects regulated entities to perform screening to all customers, stakeholders and other relevant parties at the inception of the business relationship (widely referred to as **onboarding screening**). It is also CySEC's expectation that every regulated entity must perform **ongoing screening** against all business relationships with clients, stakeholders and other relevant parties. During CySEC's thematic inspections, it was evident that regulated entities are performing onboarding screening, but the levels of ongoing screening vary greatly that requires attention in this Guidance Paper.

The main purpose of ongoing screening is to ensure that a regulated entity's **customers database remains screened against the most up-to-date information.** This is usually performed as delta screening (screening information that has changed), consisting of two main components:

- **Screening against any changes in Sanctions Lists.** In other words, every time that there is an update to a Sanctions List, the whole database is screened against such changes to the relevant list.
- **Screening against any changes in the due diligence information of clients, stakeholders and other relevant parties being screened.** In other words, if there is a change in a customer's details (e.g. change of name, change of beneficial ownership, change of directors for legal persons, etc.), then such record is screened against all required Sanctions Lists.

As a best practice, ongoing screening should be performed in automated manner on a daily basis.

Considering the high frequency of updates to global Sanctions Lists in recent times, manual screening is not considered to be a suitable option for timely ongoing screening. Some regulated entities, which formed part of CySEC's thematic inspections, did not screen their customers' database against changes to Sanctions lists. Some regulated entities were receiving

every update to a Sanctions List, yet relied on their personal knowledge of their clients in order to conduct sanctions screening. Some regulated entities though, were conducting proper screening of their full customers' database against every Sanctions List update.

A large number of regulated entities did not screen against any changes, but performed re-screening of their high-risk clients on a periodic basis, ranging from monthly to quarterly to annually. CySEC wishes to state clearly that such ongoing, or periodic, sanctions screening is not considered to be part of a risk-based approach. **It is essential that all regulated entities ensure that all business relationships are screened against relevant Sanctions Lists in real time, and that applicable measures are undertaken immediately**, if a business relationship with a sanctioned person is identified. This is a required practice in order to comply with UN Sanctions and/or EU Restrictive Measures.

CySEC therefore expects every regulated entity, as a minimum, to:

- **conduct screening with its Sanctions screening systems of its whole customer database on the occasion of every update of Sanctions Lists that the regulated entity is obliged to screen against and any other Sanctions Lists that are screening against following internal policies; and**
- **conduct screening with its Sanctions screening systems of any customer, stakeholder or other relevant parties, whose identification details changed, against Sanctions Lists that the regulated entity is obliged to screen against and any other Sanctions Lists that are screening against following internal policies.**

Screening System Management and Quality Assurance

CySEC understands that the effective and efficient screening of all Sanction Lists is a complex process. Regulated entities should utilise screening systems to perform this critical task and it is imperative that **each regulated entity understands their screening system's capacity and performance.** Regulated entities should be ensuring that:

- **All required sanctions and other data are being screened against**, including that Sanction Lists and programs are switched on, and that all links are working.
- The Sanctions lists and other data that the screening system is checking against is **up-to-date**.
- **No sanctions records are missed by the screening system.** If the screening system is missing any sanctions records, then the regulated entity must investigate and identify the reasons and take steps to mitigate any risk or have documented reasons as to why it accepts this risk and can produce evidence thereof on CySEC request.
- **The number of alerts generated by a screening system should be within the capacity for accurate processing** by the regulated entity's compliance team i.e. the number of alerts will not be an overwhelming task for the responsible personnel to process.

Some considerations are practical and unique to each regulated entity's corporate structure, business volume and customers, operational industries and other considerations. **However, the obligation to conduct screening against specified Sanctions Lists is a common requirement across all regulated entities, regardless of the above considerations.**

Testing Methodologies

The key to understanding a screening system's capabilities and limitations is through **testing**. There are two main approaches for the testing of screening systems:

- **Production Data Testing:** This method uses production data (the regulated entity's own client or transaction data) as the dataset against which system performance is tested. This is a useful test to measure the impact of tuning different system thresholds, settings and configurations against the number of alerts generated by existing customers' database/past transactions. This type of testing is measuring operational risk. It does not provide adequate assurance on compliance risks associated with the screening systems.

- **Synthetic Data Testing:** This method uses synthetic data as the dataset against which system performance is tested. By creating a test consisting of synthetic data and knowing the exact status is of each record included in the test, it allows for accurate analysis of any anomalies in the test outputs.

Applying the Synthetic Data Testing doctrine specifically to sanction screening, enables published sanctioned records to be included in a test in order to identify whether the screening system raises alerts against known sanction records. Where a system does not raise an alert against a known sanctions record (e.g. an EU-sanctioned person), a regulated entity should be able to identify each record missed and to investigate why it was missed. Once the reason for a miss is identified, the regulated entity is in an informed position to decide on the next steps.

CySEC's view is that a regulated entity cannot have a solely risk-based approach for published sanctions records that the regulated entity is obliged to screen against under UN Sanctions and EU Restrictive Measures. Exceptions may exist to this, but such exceptions, if any, would need to be well-defined, documented and supported by evidence, and must be available to CySEC immediately upon request.

A regulated entity's analysis of its screening system's effectiveness should ensure that at least one of the names returned against a sanctions record has a sufficient nexus to the sanctioned record being screened against. If a nexus does not exist, then the sanctions record should be considered as missed by the screening system and should be addressed.

CySEC acknowledges that regulated entities may, within reason, adopt a risk-based approach on its screening system's fuzzy logic matching capabilities and the levels of alerts generated by its screening system. Any such risk-based approach must be well-defined, documented and supported by evidence.

CySEC acknowledges value in both approaches for testing screening systems, namely the Production Data Testing and the Synthetic File Testing, and a best practice would be to apply both techniques.

Types of Screening Systems Testing

There are three main types of screening systems testing:

- **Assurance Testing:** This is an independent and thorough Synthetic Data Testing consisting of sanctions records, manipulated sanctions records (fuzzy logic testing, sanctioned persons' names that are slightly changed e.g. spelling errors) and non-sanctioned records (clean IDs). The test outcomes should include full analysis of the effectiveness (hits and misses) and efficiency (volume of alerts) of each dataset.

  The test size is recommended to be a minimum of 2,500 sanctions records (from applicable UN and EU Sanctions lists and other important Sanctions Lists (e.g. US), 2,500 manipulated sanctions records (from the same Sanctions Lists mentioned above) and 100 non-sanctioned records (clean IDs). Unless a good reason exists to exclude any specific type of sanctions records, the Assurance Test files should include representative amounts of individuals, entities, BICs (Transaction Screening testing only) and Dual-Use Goods (Transaction Screening testing only). For sanctions records related to individuals and entities, the testing should include all types of 'aliases' as part of the Assurance Testing.

  Documented proof of such testing and clear and detailed reports on the outcomes should be available immediately upon CySEC's request. Lack of proof documentation will imply lack of testing.

- **Iterative Testing (system tuning and optimisation):** Iterative Testing should include both Synthetic Data Testing and Production Data Testing.

  - The purpose of the Synthetic Data Testing in Iterative Testing should be to measure compliance risk and the impact of different thresholds, settings and configuration on a system's effectiveness (hits and misses) as well as efficiency (volume of alerts) on sanctions records, manipulated sanctions records and non-sanctioned records. Test size is recommended to be a minimum of 1,500 sanctions records (from applicable

UN and EU Sanctions lists and other countries important Sanctions Lists e.g. U.S.), 1,500 manipulated sanctions records (from the same Sanctions Lists mentioned above) and 100 non-sanctioned records (clean IDs).

- The purpose of Production Data Testing in Iterative Testing should be to measure operation risk and the impact of different thresholds, settings and configurations on the levels of alerts generated against the regulated entity's own client base or historic transactions data. This data informs the regulated entity on the operational feasibility of such new thresholds, settings or configurations.

CySEC notes that the **Iterative Testing is one of the best practices to optimise screening systems' performance.**

- **List Update Testing:** List Update Testing should be performed periodically or as-and-when updates to sanction lists are published. List Update Testing is done by the method of Synthetic Data Testing. The purpose is to ensure that the data that a screening system uses to generate alerts against screened data is up-to-date. List Update Testing usually consists of a varying number of newly added sanctioned records only, alternatively against full sanction lists.

CySEC notes that the **List Update Testing is one of the best practices to ensure that data sources are up-to-date.**

Conclusions

During these thematic inspections, it was concluded that the overall effectiveness and efficiency of systems used for sanctions screening by the regulated entities require improvement and several best and poor practices were detected. Individual deficiencies or weaknesses that were identified and required the implementation of remedial actions were communicated to the respective regulated entities that participated in the thematic inspections.

Proper ongoing screening as described in this Guidance Paper is **required to be performed by every regulated entity**, irrespective of its size, business activity, industry/market and other considerations.

CySEC encourages the regulated entities to **regularly assess, test and monitor their screening tools, to ensure identification of every sanctioned person (effectiveness), while keeping the numbers of 'false-positives' at low levels (efficiency).** CySEC notes that as a best practice, different testing methodologies are recommended to comprehensively assess screening tools' performance.

Each regulated entity has the ultimate responsibility for conducting continuous screening of its customers, even if this task is outsourced/relied upon to third parties.

Regulated entities should consider the supervisory expectations set out in this Guidance Paper as a benchmark, so as to avoid poor practices identified and implement best practices identified in a risk-based and proportionate manner. In doing so, regulated entities should be concerned with the risk profile of their customers and their business activities and the products/services offered to them. Where the regulated entities identify compliance gaps in their overall screening systems and controls, a remediation plan should be established with corrective measures to be implemented in a timely manner.

It is further emphasised that the sanctions screening systems used are only a part of an effective and comprehensive Sanctions Compliance Program, for which you may refer to CySEC's Guidance on Sanctions and Restrictive Measures (Section D). **Sanctions screening measures must be applied together with other control measures, such as effective due diligence measures and controls, management commitment, continuous training and awareness, sanctions risk assessment and internal policies and procedures for sanctions-related obligations**, such as freezing of funds/assets of designated persons, identifying and reporting possible sanctions violations and circumvention, etc.