LATVIJAS BANKA
EIROSISTĒMA

Guidelines for establishing and maintaining effective sanctions screening system

In 2023, Latvijas Banka conducted a thematical review to assess the effectiveness of sanction screening systems of twenty-two banking and non-banking financial institutions (hereinafter – the Thematical Review). Within the Thematical Review 45 sanctions screening systems – in-house and third-party provided – were tested, 4 of the tested systems were manual.

During the Thematic Review it was concluded that most of the institutions' IT systems used for sanctions screening can be assessed as overall effective and efficient, and several best practice examples were detected. At the same time, for all institutions certain deficiencies were identified that required implementing remedial actions.

The purpose of these guidelines (hereinafter – Market Guidance) is to inform the financial and capital market participants of Latvijas Banka's expectations regarding characteristics of an effective sanctions screening system, including quality assurance, testing, adjustment of screening systems configurations, and on using third-party vendors etc., and share observed examples of good and poor practice.

Determining requirements for sanctions screening system

In accordance with Law on International Sanctions and National Sanctions of the Republic of Latvia all financial and capital market participants shall, based on their type of activity and customer base, conduct, and document the assessment of international and national sanction risk in order to establish, assess, understand, and manage the risks of failure to enforce the international and national sanctions (hereinafter also – sanctions). Based on this assessment, institutions shall establish an internal control system for the management of the sanctions risks, including by developing and documenting the respective policies and procedures.

Sanction screening system forms a critical part of an institution's internal control system for managing sanctions risks. Sanction screening essentially refers to the process where one string of text is compared against another to detect similarities which would suggest a possible match. It compares data sourced from an

institution's operations, such as customer and transactional records, against lists of names and other indicators of sanctioned parties or locations.

However, the sanction screening system is only a part of an effective and comprehensive internal control system for sanctions risk management, and sanction screening measures must be applied together with other control measures, such as effective know your customer processes, training of employees, procedures regulating freezing of funds subject to sanctions, procedures for identifying and reporting possible sanction violations and circumvention, etc.

On the basis of their sanctions risk assessment, institutions should determine and implement such sanction screening measures that are appropriate to manage the sanction risk inherent to the particular institution. Among other, the following requirements should be assessed, justified, and documented:

- required level of automatization and sophistication for the sanction screening system;
- which sanction lists should be screened against;
- what categories of data should be screened;
- regularity and procedure for testing sanction screening system, etc.

Example No. 1 – 2: Determining sanctions lists to be screened against and determining and documenting any limitations for screening particular lists	
Good practice	**Poor practice**
The institution has carried out a comprehensive risk assessment. Institution has identified that in addition to transactions in EURO, a large proportion of transactions are made in USD and GBP currencies. Therefore, in addition to the mandatory sanction's lists – European Union (hereinafter – the EU), United Nations (hereinafter - the UN), and Latvian national sanctions lists, the sanctions imposed by U.S. Office of Foreign Assets Control (hereinafter – OFAC), United Kingdom HM Treasury (hereinafter – HMT) shall also be screened against. Additionally,	The institution is screening against the EU, UN, OFAC and Latvian sanction lists. However, the institution in its sanction risk assessment has not assessed its transaction data, i.e., currency in which transactions are made, transaction flow to different jurisdictions. In fact, a significant number of transactions in different currencies are made to United Kingdom. Therefore, without screening against HMT list, the institution might be exposed to a risk that the institution could be involved in violation or circumvention of sanctions imposed by the United

considering institutions' client base, and offered products, which include trade finance products, institution decides to develop and screen transactions against a Dual-Use Item list[1].	Kingdom, which, among other, can cause legal and reputation risks.
The institution after a thorough risk assessment concluded that due to various alternative controls screening against "*Weak Aliases*"[2] is not efficient, because the sanction screening system is generating many false positives, which is negatively affecting the efficiency of the sanction screening system, and there is a small likelihood that screening against "*Weak Aliases*" would allow the institution to identify a sanction individual/ entity, considering that there are other control measures in place to mitigate risks. Institution has identified that OFAC does not explicitly require screening against "*Weak Aliases*"[3], however, other authorities (EU and UN) has not made a clear statement about the mentioned aspect. Considering all the mentioned and taking into account various alternative controls the Institution decides not to screen against "*Weak Aliases*" and documents the decision, where the reasons for the decision are clearly stated and are justified (including with testing, where	The institution is not screening against "*Weak Aliases*"; however, the institution has not documented such decision and has not assessed associated risks with such decision. Additionally, the institution screens against a sanction list that is provided by a third-party vendor. The third-party vendor also categorizes name types of designated individuals/entities in accordance with the official sanction lists, that allows to identify which name type is a "*Weak Aliases*". However, in addition to the official categorization, the third-party vendor, in order to make the screening more effective, has developed its subjective categorization, where, based on certain principles, the third-party vendor can decide to re-categorize a name type, e.g., what in official sanction list is referred as name type "*Strong*", the third-party vendor can categorize as "*Weak*". However, the institution is not aware that the third-party vendor is performing such re-categorization of name types. Therefore, the institution is not aware

[1] Termin "Dual-Use Items" in the context of this document means goods, software and technology that can be used for both civilian and military purposes, especially used for terrorism.
[2] A "*weak alias"* or "*weak also known as*" is a term for a broad or generic alias of a sanctioned individual or entity and is included in the official sanction list that may generate a large volume of false hits when such names are run through a computer-based screening system.
[3] OFAC has stated that OFAC's regulations do not explicitly require any specific screening regime. Financial institutions and others must make screening choices based on their circumstances and compliance approach. As a general matter, though, OFAC does not expect that persons will screen for weak AKAs but expects that such AKAs may be used to help determine whether a "hit" arising from other information is accurate. See information here: | Office of Foreign Assets Control (treasury.gov)

appropriate) and relevant risks that arises from such decision are outlined.	of risks that are associated with such decision not to screen against such name types that according to official lists are "*Strong*", but according to the third-party vendor are identified as "*Weak Aliases*".

In order to determine, what level of automatization and sophistication should the sanction screening measures have, i.e., manual vs IT automatic solution, or a combination of both types, the institutions shall at least consider the specifics of the services provided by the institution, as well as the number of daily/monthly transactions and the number of customers. The institution should be able to justify that the measures it has taken to manage sanction risks are appropriate to risks that the institution is exposed to, considering institution's sanctions risk assessment.

Example No. 3 - 4: Determining the level of automatization of sanction screening system	
Good practice	**Poor practice**
The institution has carried out a sanction risk assessment and has evaluated its provided services and products, the daily/monthly number of customers' transactions, number of existing customers, intensity of new customer onboarding, and has determined that to ensure adequate sanction risk management, it is necessary to implement an automatic IT system solution for screening of both – transactions and customers. Considering limited technical capabilities of the institution, the institution decides to use a third-party service provided IT tool for sanction screening. The management of the institution understands the importance of effective sanction screening and has allocated sufficient resources necessary for the new IT tool. Institution's sanctions officer and IT specialists are involved in cooperation	The institution used to provide limited products and therefore was performing only manual sanction checks on publicly available sources, which were appropriate for managing its sanction risks. The institution has started to offer a new product. However, before implementing the new product, the institution in its targeted risk assessment for the product did not assess, whether the existing sanction screening measures will be effective to ensure management of risks inherent to the new product. In practice, after the new product was introduced, the institution's employees responsible for carrying out the manual sanction checks cannot perform the necessary tasks within time frame determined in the internal procedures of the institution, therefore creating back-logs for both - transaction monitoring

with the third-party vendor and in the implementation of the new IT solution to ensure that all the institution's determined requirements are met, and that the new IT tool is properly integrated with other institution's IT systems and is tested before implementation.	and *know-your customer* processes and leading to increased sanctions risks and customer complaints.
The institution has carried out a risk assessment and has concluded that, considering the provided services it would be disproportionate to implement automatic sanction screening for incoming/outcoming payments. The institution only offers limited range of products with has been assessed as low-to medium-low risk products, and its customer base is comparatively small. The institution has implemented additional controls, namely, its product limitations foresee that only residents of Latvia may receive the institution's services, for the purpose of receiving the service the customer shall use only an account in another credit institution that is registered in the EU, and the institution is not accepting third-party payments. Additionally, institution regularly assesses the actual payment flow, to determine whether the determined product limitations have been met in practice and sanctions risks are being managed effectively.	The institution has implemented an automated sanctions screening tool; however, its functionalities have not been evaluated in a sufficient detail. For example, the institution is not aware that the screening tool has very limited fuzzy matching algorithms, which will not ensure effective and efficient identification of manipulated sanctioned records. Thus, the functionalities of the screening tool are insufficient to ensure effective management of sanctions risks, considering the type and scale of institution's services and customer base.

Important step in setting up an effective sanctions screening system is to determine what type of data is at the institutions disposal regarding customers and transactions, so that all relevant data categories could be implemented into the screening system. If certain set of data categories are left out of the screening system, it should be justified and documented accordingly.

Example No. 5 - 6: Determining relevant data categories to be screen against	
Good practice	**Poor practice**
Upon onboarding a customer, the institution carries out a comprehensive *know your customer* process, during which, among other, the ownership structure, beneficial owner, individuals who have the power to represent the customer, and other persons connected to the customer, such as natural and legal persons within the management or ownership structure, who may be controlling/exercising a dominant influence are identified. The institution regularly screens its customer base, including the customer itself, customer's representatives, beneficial owner, and other related persons who could be capable to exercise control/dominant influence over the customer. The institution has determined and documented which data categories shall be screened against, for example, name and surname/company title, date of birth, registration number, nationality, address, etc., to ensure that the screening results provide the most accurate results. Institution ensures that the *know your customer* information remains up to date and ensures that in case of changes customer and its related persons are screened.	Upon onboarding a customer, the institution carries out a comprehensive *know your customer* process, during which all the necessary information is acquired. However, the institution regularly screens only its customers, its representatives, and customers' beneficial owners. Therefore, when a legal entity that owns the majority of the customer's capital shares is designated, the institution fails to identify that the customer's funds must be immediately frozen, because this information has been excluded from the screening system.
For transaction screening the institution has identified, which data categories shall be screened against, e.g., names of parties involved in the transaction, financial institutions,	The institution provides trade finance services and has implemented certain controls to manage risks related to sanctions. However, the institution has not defined clear procedures that

including correspondent banks involved in the transaction, free text field, address field, IP address (that is relevant to ensure compliance with sectoral sanctions applying to certain regions). The institution has taken into consideration the differences in different type of transaction messages (e.g., for SEPA and SWIFT payments).	would outline all data categories that should be screened against when trade finance services are provided. Employees, who are responsible of carrying out manual checks of the presented trade finance documentation fails to screen information about the vessel involved in the transaction (including International Maritime Organisation (IMO) numbers). Thereby, the institution fails to identify that the vessel involved in the trade finance deal has been sanctioned.

Advanced name matching technology is essential for an effective sanctions screening system, so that possible matches where data, whether in official lists or in institution's internal records, is spelled differently due to transliteration, misspelled, incomplete, or missing, could be identified. Sanction screening systems should be capable of applying fuzzy matching algorithms, i.e., an algorithm-based technique, the purpose of which is to match one name (a string of words), where the content of the information being screened is not identical, but its spelling, pattern or sound is a close match to the contents contained in a data set used for screening. Accordingly, sanction screening systems should be calibrated in a way, for example, by calibrating the percentage of fuzzy matching, so that the screening system not only will alert exact match (when an alert is generated if the system is presented with data that exactly matches a data in the screening list), but also in case certain manipulations would have been made.

The institutions should be aware that lowering the fuzzy matching percentage or altering the parameters of the algorithm will result in higher number of alerts, part of which will be false positives. Evidently, this can negatively affect the efficiency of the screening system. Therefore, the institutions should calibrate the fuzzy matching parameters in a manner that ensures both – that the system is working as effective as possible (no or minimal number of sanctions records are missed), but at the same time the screening system is working efficiently, i.e. sanction screening system is generating qualitative alerts and the screening system is not generating extensive number of false positives that could require disproportionate resources for investigation of such alerts, result in back-logs and cause series of operational risk and customer complaints. Assessment and testing should be carried out by the institutions to determine the appropriate calibration for the sanction screening system.

There are different types of fuzzy matching algorithms that could be applied. When evaluating which algorithms to apply more effectively or which algorithms to focus more on, an appropriate assessment and testing should be carried out. Table below shows commonly used fuzzy matching algorithms:

Text Matching	Text Manipulation	Word Manipulation	Date Adjustment
Soundex	Text Character Add	Word Delete	Add Subtract Date
Levenshtein Distance	Text Character Delete	Word Swapping	Swap Day and Month Date Valid
Metaphone 3	Text Character Add and Delete	Word Joining	Swap Decade of Year
	Text Character Reversing	Word Separating	
	Text Contextual Start	Word Moving	
	Text Contextual End	Abbreviation Combined	
	Text Contextual Complete	Abbreviation Combined Dot	
	Fat Finger Replace	Abbreviation Combined Space	
	Text Character Add Repetition	Abbreviation Combined Dot Space	
	Text Character Remove Repetition	Word Joining with Hyphen	
	Text Alphanumeric Swap	Word Reordering	
	Text Phonetic Character Replace	Add Initial	
	Text Character Add Special Characters	Add Initial Dot	
	Initial Letters Change	Name Duplicate	
	Add Subtract Number	Duplicated Name Remove	
	Number Add	Initial Join Space Delete	
	Number Swap	Digit to Text	
	Number Remove	Text to Digit	
		Ordinal Number Abbreviate	
		Ordinal Number Expand	

Example No. 7 - 8: Determining fuzzy matching parameters and deciding on additional controls with the aim to improve screening efficiency	
Good practice	**Poor practice**
The institution has calibrated the fuzzy matching parameters to a certain level that ensures that the screening system is working both effectively and efficiently. The parameters have been determined and validated based on comprehensive testing, where different models were tested. The institution has developed a testing environment, which is as close as possible to the institution's production environment. The testing was carried out and documented by the institution before implementing the settings in the production environment. According to the internal regulations of the institution, the institution re-assesses the determined parameters within a certain regularity and make necessary changes, which are tested and validated before implementation in the production environment.	The institution has decided to change the parameters of the fuzzy matching in order to increase the effectiveness for screening manipulated data. However, the institution has not assessed how such changes will affect the efficiency of the screening system. In the result of this decision the institution's employees are faced with significantly higher number of alerts per day. The employees cannot manage to investigate the alerts within the determined time frame in a qualitative manner, therefore alerts are closed as false positives without proper investigation.
The institution has implemented additional measures to increase the efficiency of the sanction screening system, such as whitelist, where system supresses common alerts that are false positives. The institution has clear procedures that determine the creation and usage of such list, including, how such list is reviewed, updated, amended, etc. Institution regularly assesses the effectiveness of this measure, carries out relevant testing and implements appropriate changes, when necessary.	The institution has implemented additional measures to increase the efficiency of the sanction screening system, i.e., whitelist. However, as the institution does not have clear procedures that regulate the usage of such list, the institution has not included the whitelist in the scope of data that the institution should regularly screen against that would allow to identify instances when the list should be reviewed and updated. Therefore, for example, if a new sanction regime has been imposed, institution now is exposed to risk that the whitelist contains data that should potentially generate a positive match.

The main aspects of sanctions screening system that should be regularly assessed and monitored

Considering the results of the Thematical Review and noting the importance of effective sanction screening measures, it is imperative that each institution regularly assesses, understands, monitors, and improves their screening system's performance. This includes assessment of the following aspects:

- all required sanction lists are being screened and all sanction regime programs are "switched on" and are working correctly (e.g. EU sanction regime against Russia, EU terrorist list, etc.);
- all relevant data categories (i.e., all customers, relevant customers' associated parties, other data categories, such as IP addresses, etc.), transaction fields (i.e., payer, payment receiver, financial institutions involved in the payment, transaction's description/free text field etc.) are being screened against;
- the sanction lists and other data that a system is screening against is up to date and correct;
- low or zero sanctioned records are being missed by the system; if the screening system does miss sanctioned records (client/transaction screening), then the institution must be aware of the reasons for this, have taken steps to assess and mitigate any risk, and have documented reasons why this risk can be accepted (e.g., institution decides not to screen against "weak aliases" or decides not to screen against dual-use item lists);
- the institution's sanction screening systems together with other controls for ensuring data quality (e.g., measures to ensure quality of institutions' customers' data, for example, that a customer cannot be on-boarded if date of birth or other identification data is missing) are capable of fuzzy matching, i.e., effectively identifying possible sanctioned record when manipulations or typos, including, word and date manipulations have been made;
- the screening system is working efficiently, i.e., the sanction screening system is generating qualitative alerts, and the screening system is not generating extensive number of false positives, including for non-sanctioned records;
- the institution has sufficient resources for processing and investigation alerts qualitatively and within the set time limits, i.e., the number of alerts that must be processed does not cause operational risks that can result in

back-logs or lowered quality of transaction monitoring or *know your customer* processes.

Common reasons for ineffective or inefficient sanction screening system

Generally, if a screening system is not performing as expected, it might be because of one, or a combination of the following reasons:

- inappropriate configuration (e.g., only exact, or almost exact matches of sanctioned records will be alerted by the screening system)
- efficiency of sanctions screening system is not assessed together with the systems' effectiveness. In the result the system might be very effective for screening control and manipulated sanctioned records, however, the number of false positives is too excessive and therefore the system is not efficient, causing operational risks; or vice versa – the system is performing very efficiently with small number of false positives; however, the system is ineffective for screening manipulated records;
- over-reliance on technological solutions and third-party vendors where the institution has a limited understanding of its sanction screening systems' configurations;
- the screening system is being used with "out-of-the-box" or factory settings without adapting it to the specifics and risks of the institution;
- the sanctions screening system's version, rules and/or settings have not been updated in a reasonable time frame or after significant changes in sanctions regulations;
- the external list provider is not fully up to date;
- there are problems with the institutions' list feed in keeping up with the list providers updates;
- list management – too many or too little sanction sources are being screened against;
- testing of IT system has not been performed or the scope of testing has been too limited;
- no testing environment has been developed or the testing environment significantly differs from the production environment, or there are no clear testing procedures;

- poor involvement of the anti-money laundering (hereinafter – AML) and sanctions risk management teams in setting up and/or maintaining sanctions screening systems;
- deficiencies in change management processes, e.g., sanction screening system technical aspects are not considered when changes in other institutions' processes take place;
- insufficient support from management in the implementation, improvement, and testing of sanction screening systems.

Testing Methodologies

The key to understanding a screening system's abilities and challenge areas is engagement with and testing of the screening system. There are two main approaches to testing of sanctions screening systems.

1. **Production Data Testing**: this method uses production data (institution'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 different thresholds, settings, and configurations on the number of alerts being generated against institution's existing database/past transaction. This type of testing measures operational risk. This type of testing does not provide adequate assurance on compliance risks associated with screening systems.

2. **Synthetic Data Testing**: this method uses synthetic data (artificially generated data that mimics the characteristics of real-world data but is not derived from actual, existing records) as the dataset against which system performance is tested. By creating a test consisting of synthetic data and knowing exactly what the status is of each record that is included in the test, it allows for accurate analysis of any anomalies in the test outputs.

Applying the Synthetic Data Testing method to sanction screening, published sanctioned records are included in a test to identify whether or not the screening system raises alerts against known sanction records. Where system does not raise an alert against a known sanction record, an institution is then in a position to identify which record was missed and investigate the reason, and take informed steps on making necessary improvements to the screening system. There is different value and metrics in both Production Data Testing and in Synthetic File Testing, and therefore it is best practice to apply both techniques while testing effectiveness and efficiency of sanctions screening systems.

Institution's analysis of its screening system's effectiveness should include ensuring that at least one of the names returned against a sanction record has a

sufficient nexus (i.e. link) to that sanctioned record being screened against. If a nexus does not exist, then a sanction record should be considered as missed by the screening system and should be addressed by the institution.

Institutions 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.

Testing Types

Three main types of screening system testing can be distinguished:

1. **Assurance Testing** – independent and thorough Synthetic Data Testing consisting of sanction records, manipulated sanction records (fuzzy logic testing) and non-sanction records. Test outcomes should include full analysis of the effectiveness (hits and misses) and efficiency (level of alerts) of each dataset. The minimum data size of test should be statistically significant, also taking into account the institutions size and nature, and should include sanctions records from official lists and additional lists, if any, according to the institution's risk assessment, as well as manipulated sanctions records and non-sanctioned records. In line with international good practice the minimum data size is 1 500 test records. Assurance Testing files should include representative amounts of individuals, entities, BICs (Transaction Screening testing only) and Dual-Use Items (Transaction Screening testing only), unless there are good and justified reason to exclude a specific type of sanctions records. As it relates to individuals and entities, tests should also include all types of aliases as part of Assurance Testing.

Institutions should implement appropriate (self -testing or independent testing by using outsource service providers, who have the necessary experience and competence to conduct such tests). Assurance Testing in the following instances:

- regular testing, according to internally set regularity, but at least once per each 18 months, while assessing the effectivity and efficiency of the operation of the internal control system, including sanction screening system. In line with international good practice it is recommended to perform testing once per 12 month;
- when a new screening system is implemented;
- when a major system update or upgrade is implemented in production;
- when an existing system's settings and/or configurations are changed significantly in production.

Testing results with clear, detailed reports should be documented and used for assessment of the effectiveness of internal control system for sanctions risk management.

2. **Iterative Testing** – system tuning and optimisation, and should include both Synthetic Data Testing and Production Data Testing. This testing type is aimed to assess and optimise the performance of institution's screening system.

The purpose of the Synthetic Data Testing in Iterative Testing is 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 (level of alerts) on sanctioned records, manipulated sanctioned records and non-sanction records. Test data size should be appropriate to the institutions size and nature, and include sanction records from the sanction lists that institutions are required to screen against, as well as additional lists, if any, according to institution's risk assessment), manipulated sanction records and non-sanctioned records.

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 institution's own client base or historic transaction data. This data informs the institution on the operational feasibility of such new thresholds, settings, or configurations.

3. **List Update Testing** – this testing type helps ensure that data sources are up to date. List update testing is recommended to be performed periodically or as-and-when updates to sanction lists are published, and usually is done by Synthetic Data Testing. List update testing usually consists of a varying number of newly added sanctioned records only, alternatively against full sanction lists.

Reliance on Third Parties

If an institution uses third party solutions for the sanctions screening, it should be noted that blind reliance on the capabilities of external provider is not acceptable. Each institution is responsible for ensuring the effective management of sanctions risks, regardless of whether an in-house or external solution is used for sanctions screening.

Example No. 9: cooperation with third party service providers	
Good practice	**Poor practice**
The institution has developed policies/procedures for regularly monitoring the activity of the third-	The institution completely relies on a third-party vendor for the sanction screening. The institution's sanction

party vendor that provides the institution with the sanction screening tool, which also include regular inspections and sample testing. Among other, the tests include how quickly and effectively the third-party vendor implements the new sanctions amendments/regimes, whether the sanctions lists include all required mandatory lists. What algorithms does the service provider use to capture manipulated data and how effectively they work. When the institution concluded the contract with the third-party vendor, it ensured that the contracts also include requirements for system improvement measures, including system improvements based on the institution's risks, specifics, and suggestions.	team has insufficient understanding of how the IT system works, what data sources are used, how new sanction records are detected and how quickly they are incorporated into the system, including which sanction records (e.g. alias types) are considered.

Conclusion

This best practice guidance emphasizes the importance of effective sanction screening measures and outlines good practice expectations for financial and capital market participants to successfully comply with regulatory enactments regarding sanctions risk management. Institutions are required to conduct regular risk assessments, document their sanction screening system configurations and testing results, and implement measures appropriate to their specific risks. It is important to remember the need for a holistic approach, combining sanction screening settings with other control measures like effective know your customer processes, employee training, and procedures for freezing funds subject to sanctions, etc.

Furthermore, Thematic Review highlighted common reasons for ineffective screening systems, including inappropriate configuration, lack of updates, and poor involvement of AML and sanctions risk management teams in setting up, testing, and maintaining sanctions screening systems. Therefore, Latvijas Banka encourages institutions to regularly assess, test and monitor their screening systems, ensuring they effectively identify sanctioned records while minimizing

false positives. Different testing methodologies are recommended to comprehensively assess system performance.