

Elevate AML Compliance with Name Screening Software



Sanctions checks have been a regulatory requirement for the following in the UAE:

- Designated Non-Financial Businesses and Professions (DNFBPs)
- Virtual Asset Service Providers (VASPs)
- Financial Institutions (FIs)

Anti-Money Laundering (AML) compliance is impossible without reliable sanctions screening software. Let's explore how regulated entities can elevate their AML compliance with name-screening software.



TABLE OF CONTENT

What is Name Screening	01
How Name Screening helps fight ML/FT	02
Name Screening: Legal and regulatory landscape	13
Name Screening Process	23
Best Practices in Name Screening	32
Name Screening Software Features	45
Types of Watchlists Used for Name Screening	54
Importance of Name Screening Software	59
Challenges in Sanctions Screening	62
Best Practices in Sanctions Screening Software Implementation	69
Conclusion	79
FAQs	82
About RapidAML	91

A large, stylized purple arrow graphic pointing to the right, composed of several parallel lines of varying shades of purple, located on the left side of the page.

WHAT IS NAME SCREENING

The exercise of matching a list containing names of customers, suppliers or business partners against the sanction lists, watchlists, or databases issued by regulatory authorities of various countries or international organisations is known as name screening.

Name screening can be carried out either using software, APIs, automated screening tools, or manually searching names across sanction lists.



HOW NAME SCREENING HELPS FIGHT ML/FT

To understand how name screening works and helps in fighting money laundering (ML), terrorism financing (TF), and proliferation financing of weapons of mass destruction (PF), it's important to know:

Which “Sanction Lists”

Whose “Names”

When to “Screen”



Basics of Name Screening



WHICH lists to screen names against?

UAE local terrorist list, UNSC consolidated list, PEP list, adverse media, and other relevant lists as per the risk-based approach taken by the regulated entity.



WHOSE names to screen?

Potential and existing (legal/natural persons) customers, suppliers or business partners.



WHICH lists to screen names against?

At the time of onboarding new customers, before making a transaction, and ongoing screening of customers, suppliers, and third-parties.

Additional Information



Video

How Name Screening Helps in Fighting Money Laundering and Terrorist Financing



Which Sanction Lists to screen names against?

As per UAE AML/CFT laws and regulations, regulated entities are required to consider UAE local terrorist list and UNSC consolidated list to comply with their legal obligations.

However, DNFBPs, VASPs, and FIs dealing with foreign customers should take into account other relevant lists as per the risk-based approach taken by them.





Whose names to screen across the aforesaid Sanctions List?

Potential and existing customers (legal or natural persons), suppliers or business partners and their directors, Ultimate Beneficial Owners (UBOs), authorised signatories, and representatives through the power of attorney. In case of a minor as a customer/ supplier or business partner, their parents or legal guardian need to be screened.





When to screen?

At the time of onboarding, i.e., establishing a business relationship or while continuing a business relationship, before making a transaction, and ongoing screening of customers, suppliers, and third parties. Re-screening existing customers when there is a change in their Know Your Customer (KYC) information.





Name screening is carried out for various purposes, particularly to identify sanctioned or politically exposed individuals or entities while carrying out regular business activities to prevent onboarding such individuals or entities as their customers, suppliers, or business partners.

The need to avoid onboarding such individuals or entities arises from the requirement to stop or restrict such individuals or entities from entering or establishing their foothold in the legitimate financial system.





The process of carrying out name-screening exercises helps businesses to stay compliant with anti-money laundering (AML), counter-financing of terrorism (CFT) and counter-proliferation financing (CPF) of weapons of mass destruction laws.

They also need to comply with regulations around the world and directives, recommendations, findings and interpretive notes of international organisations such as the Financial Action Task Force (FATF), United Nations Security Council Resolutions (UNSCRs) related to the sanction regimes as UAE is a member of United Nations; thus, compliance with UNSCRs is required and various local UAE laws.





The role of Sanctions Check in financial crime prevention

Sanctions are restrictive or prohibitory measures taken by countries either single-handedly or jointly with the primary goal of requiring deterrent or non-compliant individuals, organisations or countries to change their status of non-compliance with AML laws towards compliance.

The UAE laws and various international sanctions regimes are enacted with the intention of safeguarding economies being used as channels to circulate illicit proceeds and fund terrorist activities. To enable businesses to steer clear of criminals and organisations that are suspected, blacklisted and found responsible for ML, FT, and PF, the UAE government and various international bodies have come up with lists containing names of individuals and organisations to be avoided and reported to the (Financial Intelligence Unit) FIU.





Some of the popularly used sanctions lists are:

UAE local terrorist list

UNSC consolidated list

The European Union list

The UK HM Treasury list

The United States of America's Office of Foreign Assets Control (OFAC) list



Further, UAE laws and international resolutions require businesses to adopt sanctions compliance programs. These programs usually require businesses to cross-verify the names of their existing and potential customers, suppliers, and business partners across names in such lists applicable to the business.






The prevention of ML, FT, and PF becomes possible when businesses cross-verify their existing and potential customers, suppliers, and business partners across such lists and report matches to the FIU.

When business finds a complete match or a partial match, they are required to:

- ▶ Terminate or suspend transactions
- ▶ Freeze funds and submit a Funds Freeze Report or a Partial Name Match Report as the case requires with such individuals or organisations

Thus breaking the chain or stopping them from entering legitimate financial systems.



A large, stylized purple arrow graphic pointing to the right, composed of three parallel lines of varying shades of purple, located on the left side of the slide.

NAME SCREENING: LEGAL AND REGULATORY LANDSCAPE

When it comes to the regulatory landscape in the UAE, the UAE government has enacted the various laws to prevent money laundering, terrorism financing, and the proliferation of weapons of mass destruction which we are going to discuss in this section.



Name Screening: Legal and regulatory landscape

1

Federal Decree-Law No. (20) of 2018 on Combating Money Laundering Crimes, the Financing of Terrorism, and the Financing of Unlawful Organisations.

2

Cabinet Decision No. (10) of 2019 On the Implementing Regulation of Federal Decree-Law No. (20) of 2018 on the Criminalisation of Money Laundering and Combating the Financing of Terrorism and the Financing of Unlawful Organisations.

3

Cabinet Decision No. (74) of 2020 Concerning the UAE List of Terrorists and the Implementation of UN Security Council Decisions Relating to Preventing and Countering Financing Terrorism and Leveraging Non-Proliferation of Weapons of Mass Destruction, and the Relevant Resolutions.

- ▶ Particularly requires financial institutions, DNFBPs, and VASPs to subscribe to the mailing list maintained by the Executive Office for Control and Non-Proliferation (EOCN), screen customers and transactions, apply adequate TFS measures like fund freezing, and report to the authorities.
- ▶ Taking TFS measures and making it impossible for individuals or organisations from securing funds, assets or economic resources to proceed with their illicit intentions.

4

Guidance on Targeted Financial Sanctions for Financial Institutions, Designated Non-Financial Businesses and Professions and Virtual Asset Service Providers.

5

Other Laws, Regulations and Guidelines issued by various supervisory authorities across the UAE, such as:

- ▶ FSRA - Financial Services Regulatory Authority, for Abu Dhabi Global Market (ADGM)
- ▶ DFSA - Dubai Financial Services Authority, for Dubai International Financial Centre
- ▶ VARA - Virtual Assets Regulatory Authority for Virtual Assets Service Providers (VASPs) in Dubai



Regulatory requirements around Sanctions Screening for DNFBPs and VASPs

Broadly speaking, the aforementioned laws in UAE and the Guidance on Targeted Financial Sanctions for Financial Institutions, Designated Non-Financial Businesses and Professions and Virtual Asset Service Providers cover the major obligations of DNFBPs and VASPs.

Some of these obligations revolve around ensuring that a proper process is followed to carry out sanctions screening.

Additional Information



Infographic
Step-By-Step Guide to Sanction Screening



TFS Requirements

Draft Policies & Procedures

Drafting and implementing policies, procedures, and internal controls to ensure compliance with Cabinet Decision No. 74 of 2020

Subscribe to EOCN Mailing List

This step requires DNFBPs and VASPs in the UAE to subscribe to the EOCN Notification System on the EOCN's website to receive automated emails regarding updates to the sanctions list. This will help VASPs and DNFBPs freeze and unfreeze individuals or organisations on the list in a timely manner

Perform Screening

DNFBPs and VASPs are required to carry out frequent and regular ongoing screening on the Local Terrorist List and the UN Consolidated List before onboarding new customers and at the time of change in customer information during KYC of the existing customer and before carrying out any transaction



Apply TFS Measures

Measures included are:

- ▶ Freezing funds or assets without delay
- ▶ Prevention of making funds, assets, or services available

Submit Regulatory Reports

Calls for reporting of TFS measures taken through the goAML portal by filing:

- ▶ Funds Freeze Report (FFR)
- ▶ Partial Name Match Report (PNMR)
- ▶ Reporting Suspicious Transactions Reports (STRs) / Suspicious Activity Reports (SARs) when TFS-related red flags are seen

Co-operate with Authorities

Coordinate with the relevant supervisory authority



International Standards: FATF Recommendations

The FATF is a global AML, CFT, and CPF watchdog that makes suggestive recommendations to prevent ML, FT, and PF acts and sets international standards for harm caused by these illegal activities to society.

The standard set out by FATF ensures a coordinated global response in preventing ML, FT, and PF-related crimes. They work with different authorities and help them detect and deal with criminal acts.

Additionally, it lists countries on black and grey lists to help them out with policies to prevent ML, FT, and PF activities that harm the integrity of the international financial system.





FATF Recommendation 6

FATF Recommendation 6 deals with the Targeted Financial Sanctions related to terrorism and terrorist financing. It requires each country to implement TFS measures to comply with the UNSC resolutions that require countries to freeze, without delay, the funds or other assets and to ensure that no funds and other assets are made available to or for the benefit of designated person or entity by the UNSC under Chapter VII of the Charter of the UN, as required by the Security Council resolution 1267 (1999) and its successor resolutions; or any person or entity designated by that country pursuant to Security Council resolution 1373 (2001).





FATF Recommendation 7

FATF Recommendation 7 deals with Targeted Financial Sanctions related to Proliferation. It requires countries to implement TFS measures and freeze, without delay, the funds or other assets of, and to ensure that no funds or other assets are made available to, and for the benefit of, designated individuals and entities by the UNSC under chapter VII of the Charter of the United Nations, pursuant to Security Council resolutions that relate to the prevention and disruption of the financing of proliferation of weapons of mass destruction.





Name Screening is a key component of AML KYC

Businesses operating in the UAE are required to carry out AML (Know Your Customer) KYC. The KYC process forms part of RBA, where customer identification and verification are carried out.

As a part of finding risk associated with customers, it is essential to screen customers prior to onboarding them across:

Applicable and relevant sanctions lists, watchlists, and PEP lists

Media to find if any negative or adverse finding connects them to larger crimes like ML, FT and PF



- ▶ Name screening is to be carried out,
- ▶ The results or outcome of name screening is derived.
- ▶ Types of Screening Outcomes and the required action are listed below.
 - Screening Outcome No.1: “No Matches”
 - Required Action: The regulated entity can establish a business relationship with such a customer.
 - Screening Outcome No. 2 “Partial Match”
 - Required Action: For such a customer, the regulated entity needs to file a Partial Name Match Report (PNMR) with the Financial Intelligence Unit (FIU) on the goAML portal to fulfil regulatory reporting requirements. The regulated entity then needs to suspend the business relationship or transaction with a such customer until the FIU gives instructions.
 - Screening Outcome No. 3 “Complete Match”
 - Required Action: The regulated entity needs to file a Fund Freeze Report (FFR) with the FIU goAML portal and terminate the business relationship with such a customer. Name screening is interwoven with the process of conducting KYC and implementing a risk-based approach.



NAME SCREENING PROCESS

The Name Screening process is carried out by entering key identifiers of a natural or legal person, such as name, date of birth, aliases, nationality, ID or passport information, and last known address for a natural person and business name, aliases, address of registration, address of branches, and other relevant information for a legal person into the sanctions screening tool when relying on technology for name screening or manually cross-verifying these identifiers across the sanctions list or watchlists applicable to the regulated business carrying out name screening.



Essential Identifiers for Name Screening



Natural Person

- ▶ Name
- ▶ Aliases
- ▶ Date of Birth
- ▶ Nationality
- ▶ ID or Passport Information
- ▶ Last Known Address



Legal Entity

- ▶ Trade/Business Name
- ▶ Aliases
- ▶ Address of registration
- ▶ Address of branches
- ▶ Other Information

Additional Information



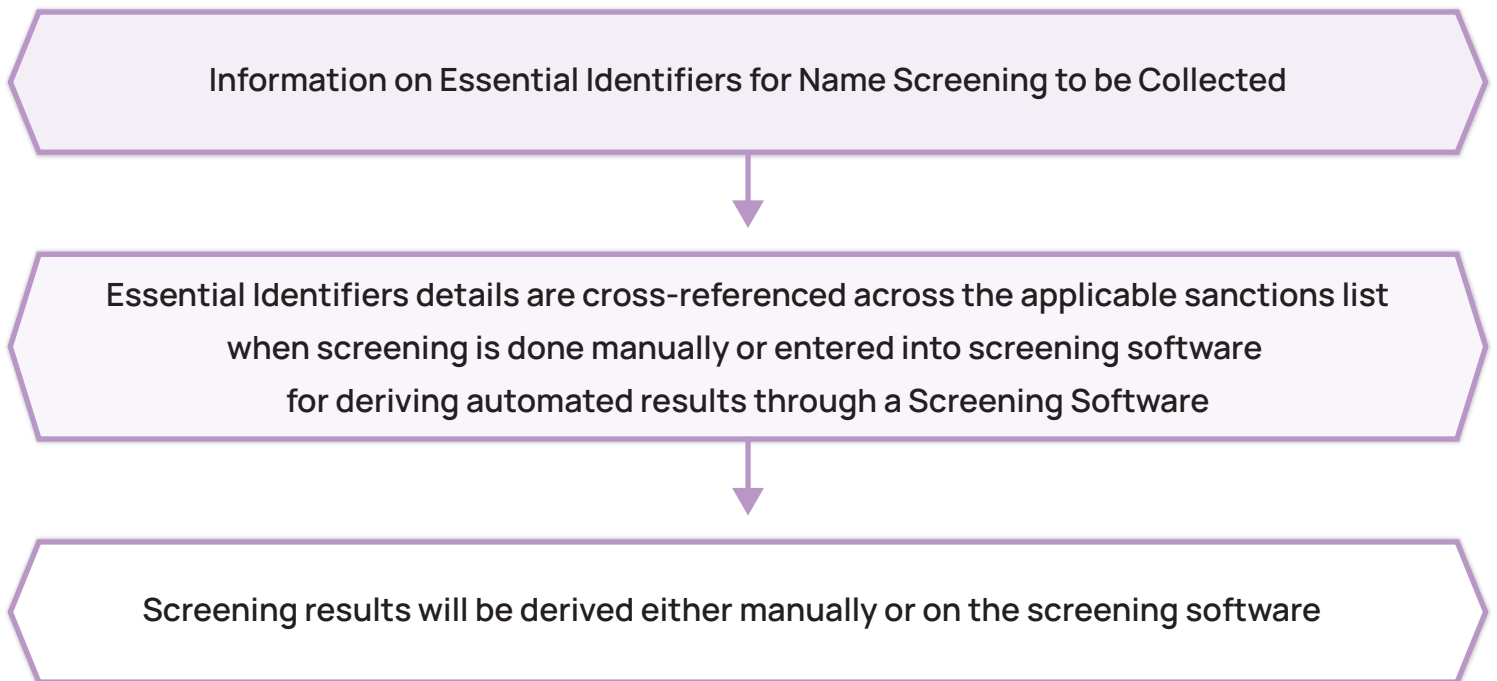
Infographic

The orderly process of customer screening to ensure AML compliance



Sanctions Screening Process

The Sanctions Screening process is generally carried out by taking the following steps:



Additional Information



Video

The Orderly Process of Customer Screening to Ensure AML Compliance



The result of name screening would show the following results, with interpretations of each one explained below:

Confirmed Match

Interpretation:

Person/Entity who is being screened has their name on the sanctions list or watchlist.

Probable Outcome:

Then, such a person/entity could be a designated person/entity.

Action Required:

- ▶ Immediate reporting to the UAE Financial Intelligence Unit (FIU) in the form of a Funds Freeze Report (FFR).
- ▶ Apply freezing measures on the assets and funds available with the business within 24 hours.
- ▶ Avoid conducting business or providing service to such a designated person/entity.

Best Practice:

- ▶ Avoid tipping off or informing the person/entity about the outcome of screening results, freezing and reporting measures.
- ▶ Organising regular personnel training with regards to handling screening results.



Partial Match

Interpretation:

Person/Entity screened has a partial name match result across the sanctions list or result of screening is not conclusive as to a complete match, then such a situation results in Partial Match results.

Action Required:

- ▶ The business to suspend its transactions or business relations and report to the UAE FIU in the form of a Partial Name Match Report (PNMR).

Best Practice:

- ▶ Avoid informing or tipping off the person/entity about screening results, and PNMR measures taken.
- ▶ Conducting regular training to make the personnel aware of measures to be taken when there is partial match.

No Match:

Interpretation:

The person/entity that screened does not appear to have their name in the sanctions list or watchlists.

Action Required:

- ▶ Conduct customer onboarding as usual as is safe to conduct business.
- ▶ There are no reporting obligations to any of the regulators or the FIU in the event of No Match.

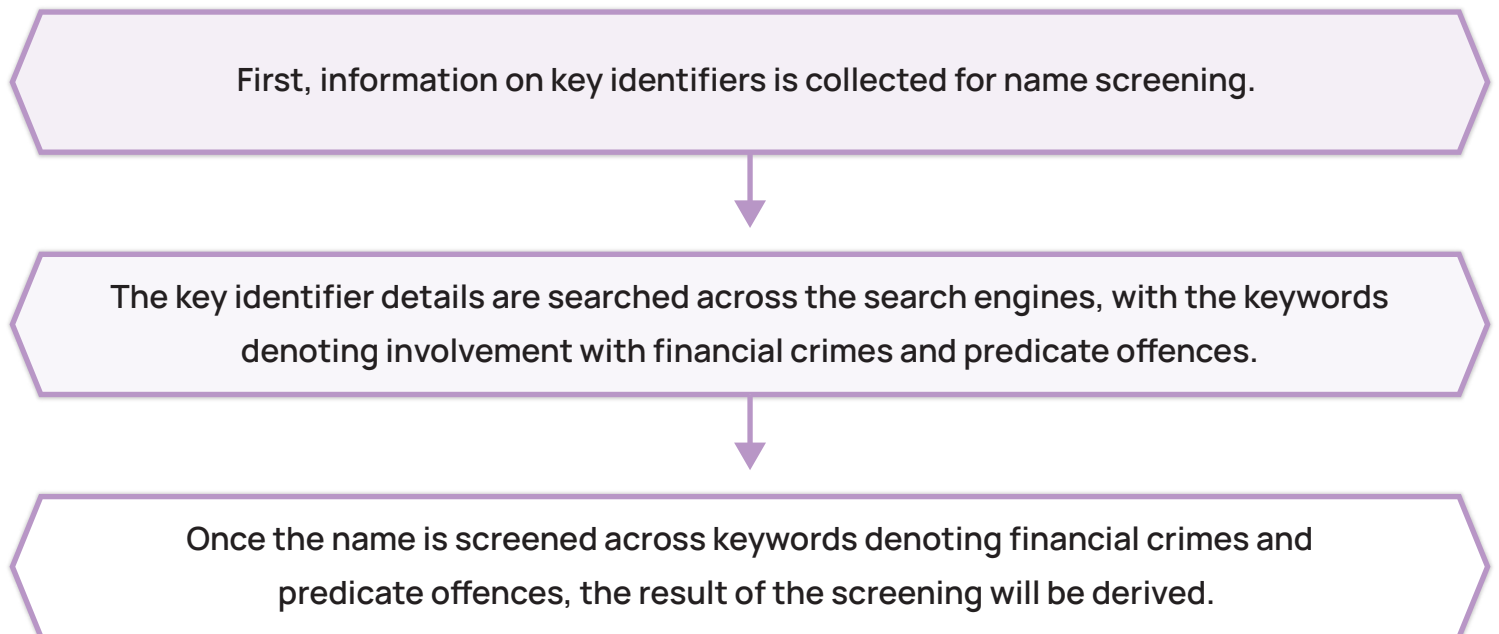
Best Practice:

- ▶ Continue with the customer due diligence requirements.



Adverse Media Screening Process

The Adverse Media Screening Process is generally carried out by taking the following steps:





The result of name screening for adverse media would show the following results, with interpretations of each one explained below:

Match Found:

Interpretation:

Person/Entity screened has their name associated with financial crimes and predicate offences.

Action Required:

- ▶ Enhanced Due Diligence measures need to be implemented to ascertain the true extent of risk they pose to the business.
- ▶ Submit a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) in case of suspicion as to Money Laundering or Terrorist Financing.

No Match/False Match:

Interpretation:

that was screened for negative news does not appear to have their name associated with keywords that denote involvement with financial crimes and predicate offences.

Action Required:

- ▶ It is safe to conduct business as usual.



Politically Exposed Person (PEP) Screening Process

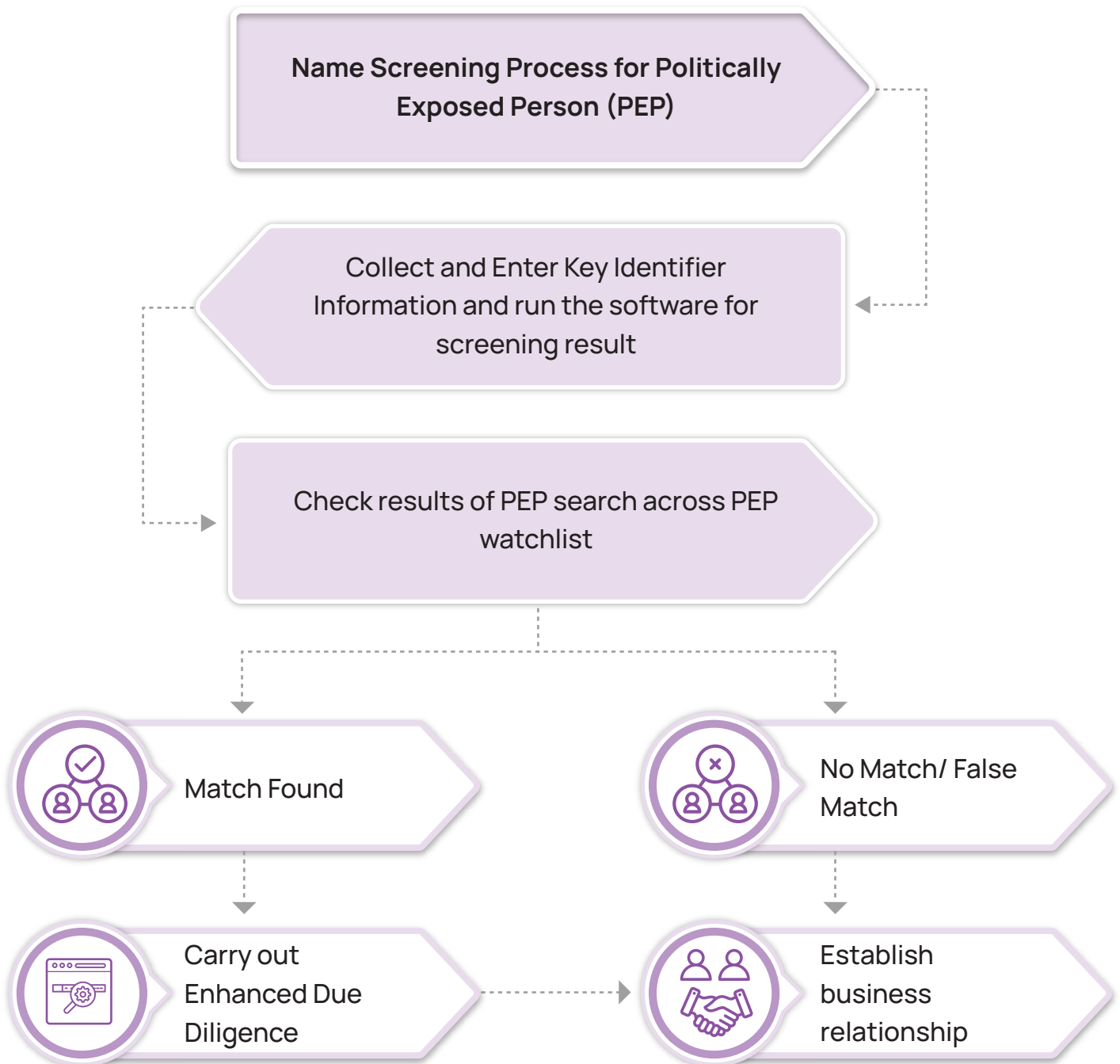
PEP screening is required to identify if a potential customer, supplier, or business partner is a Politically Exposed Person (PEP), meaning that such a person holds political influence. PEPs are generally categorised as high-risk due to their reach and influence. When a customer is identified as a PEP, enhanced diligence measures need to be applied.


The process of PEP screening entails entering key identifier data into screening software or across a PEP watchlist. The screening result determines whether a customer is PEP.





Politically Exposed Person (PEP) Screening Process



A large, stylized arrow graphic on the left side of the page, composed of three overlapping, semi-transparent purple chevron shapes pointing to the right.

BEST PRACTICES IN NAME SCREENING

Given the need for name screening for better compliance with the AML regulatory framework, it is necessary that businesses be familiar with best practices in name screening to ensure that their obligation under the AML framework is delivered in an effective manner.



Best practices around the name screening process include the following measures that a business can undertake.





1. Applying a risk-based approach

The FATF recommendations and UAE local laws require businesses operating in the UAE to implement a risk-based approach, where the business shall apply measures to prevent ML, FT and PF in proportion to the risks identified.

While implementing such RBA measures, risk factors pertaining to the customer need to be carefully considered. Appropriate policies, particularly sanction compliance programs, must be drawn up to adequately identify customer risk and implement commensurate mitigation measures. Such a sanctions compliance program must contain the stepwise procedure to be followed by the business's personnel while carrying out the name screening to identify sanctioned, politically exposed individuals and organisations.

The Sanctions Compliance Program must also specify the sanctions list the business will adhere to and mention the frequency of updating such lists.





2. Designing & implementing appropriate policies & procedures

The FATF recommendations, UAE federal laws & various supervisory authorities across UAE, such as the FSRA, DFSA & VARA, strongly recommend businesses have in place appropriate policies & procedures in place that clearly state and direct the steps to be taken to ensure compliance with screening requirements, including sanctions compliance program as discussed above and use of technology, reliance on third parties for carrying out screening, etc. to maintain clarity & compliance at the same time.

It's important to have a clearly drafted client exit policy in place that helps the business's employees understand how and when to reject, terminate or suspend transactions & services, particularly due to name screening results with potential and existing customers, suppliers, & business partners to ensure that the business stays within its risk appetite while conducting business.





3. Use of technology

Various supervisory authorities across the UAE now recommend relying on technology, i.e., software and APIs, to carry out sanctions screening, PEP screening, and Adverse Media screening. Implementing the correct technological tool is highly advisable as it reduces the occurrence of errors while carrying out manual screening and saves cost and time to a great extent.

Additional Information



Article

Elevate AML Compliance with Name Screening Software



4. Exploring and applying third-party services

Various supervisory authorities across the UAE also mention in their guidelines that businesses can depend on third-party solutions for getting their customer due diligence measures carried out on their behalf to meet regulatory requirements and reduce the burden of hiring staff just for meeting CDD requirements. Businesses need to be mindful that the third-party entity is following AML compliance measures up to the standards of those prescribed by the FATF and the relevant supervisory authority, and in the event of ambiguity, the stricter law shall prevail.





5. Exploring and using suitable APIs

APIs are application programming interfaces. In simple words, APIs are software intermediaries that enable two applications/software to communicate with one another seamlessly using protocols. For example, the share market app on your mobile phone communicates with the systems of the stock exchanges and gives out immediate, accurate and exact information about changes in share prices instantly on your phone.

The API for screening shall help businesses keep the sanctions database updated. Selecting a suitable API depends on a business's individual needs.





6. Staying updated with regulatory changes

The businesses operating in UAE, to ensure continuous and non-redundant compliance with sanctions and screening requirements, need to stay updated with the latest and frequent regulatory changes to ensure compliance with the ever-evolving legislative landscape. The Compliance officer and senior management must remain mindful of such updates.





7. Ongoing screening

Needless to mention, screening is not a one-time exercise; the purpose of screening would instantly get defeated when an individual or organisation screened and onboarded today with simple due diligence becomes politically exposed or ends up having their name appear on the local terrorist list tomorrow without being subject to enhanced due diligence or freezing and reporting measures. To avoid such a lapse, it's important to screen potential and existing customers, suppliers and business partners on a daily basis by way of ongoing monitoring across relevant sanctions lists.





8. Language variation consideration

Generally, international sanctions lists contain names of Arabic, Cyrillic, and Russian origin, and the language difference leads to complications when trying to match names in such lists with names in English script. The accuracy of results suffers. To remove the issues arising due to language variation, the best practice can be adopted by relying on software that uses fuzzy matching algorithms so that matching names with sanctions lists becomes possible without missing names due to language variation and leaving less room for errors in match results.





9. Testing and auditing screening measures applied

The responsibility of regulated entities does not end by subscribing to EOCN notifications or buying screening software. Businesses need to test the efficacy of screening systems and mechanisms chosen for their organisation and make sure that the measures applied are commensurate and optimum for their needs. Auditing of measures in place is essential to ensure ongoing compliance with applicable laws.





10. Selecting suitable screening software

There are many tools available in the market to aid businesses in implementing name screening. However, businesses need to be mindful that the software they select for this purpose actually suits their individual business and ensures regulatory compliance. Finding software that is a good match, affordable and compliant with the needs of the business is essential best practice; otherwise, implementing software would be a futile exercise.





11. Regular training

Employees, compliance officers, and senior management need to be trained on a regular basis to ensure that they are aware of best practices regarding name screening and its regulatory and compliance requirements to avoid criminal and administrative fines and penalties.



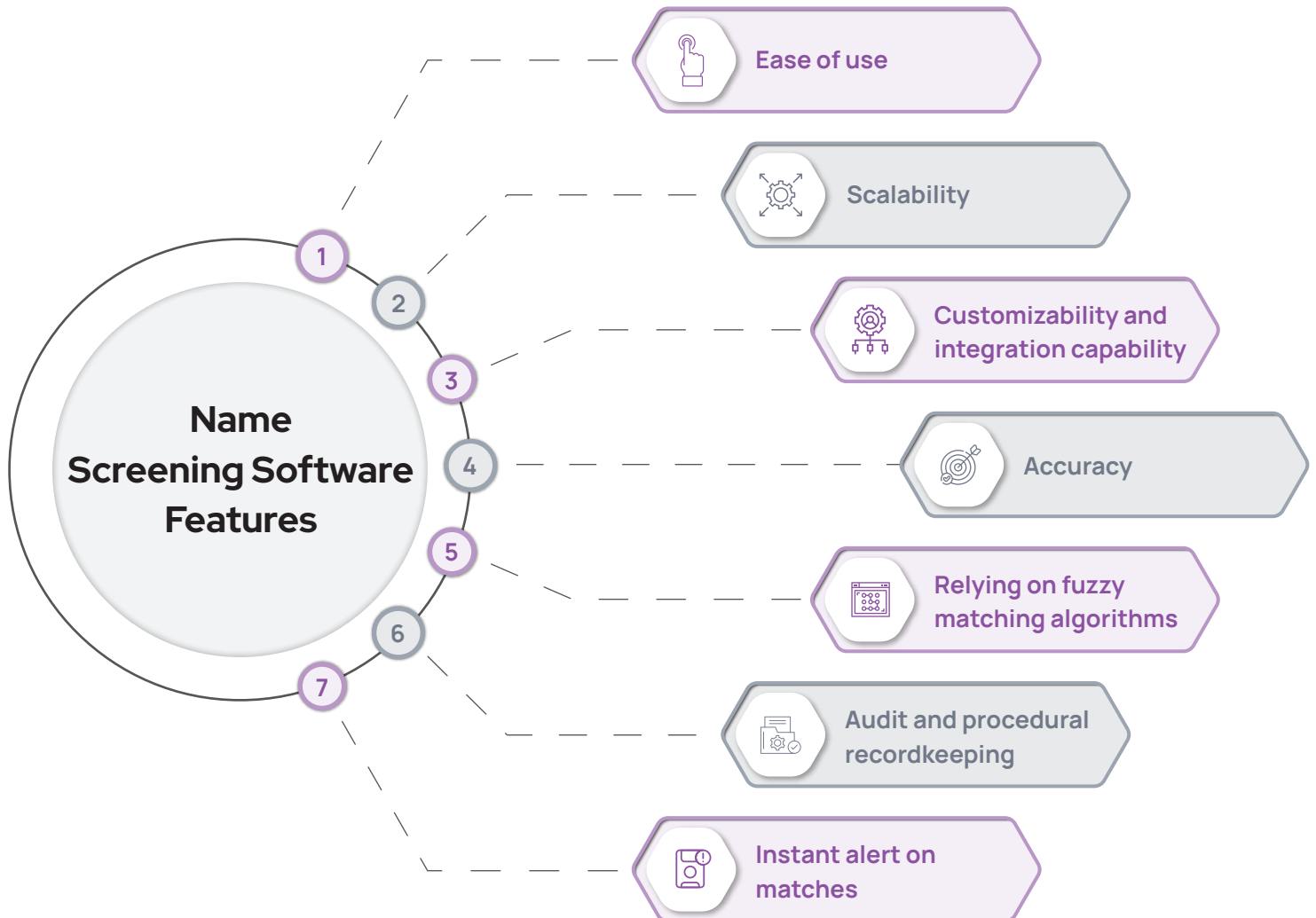
A large, stylized arrow graphic on the left side of the page, composed of three overlapping, semi-transparent purple chevron shapes pointing to the right.

NAME SCREENING SOFTWARE FEATURES

Name-screening software is generally considered a one-stop solution for fulfilling name-screening needs (sanctions, adverse media, PEP and terrorist name screening) and related regulatory compliance.



The features that make name screening software a preferred screening solution are:





1. Ease of use

Relying on any software is intended to achieve convenience and ease while carrying out tedious, repetitive, and monotonous tasks. Name-screening software solves the pain of the manual name-screening process for businesses by providing features such as bulk screening or batch screening, where hundreds of customers can be screened across various watchlists in a matter of minutes.





2. Scalability

Any good name-screening software would allow businesses to increase screening volumes, helping them achieve scalability with growing businesses.





3. Customizability and integration capability

Many good name-screening software providers offer the feature of customising or tailoring the software to suit the needs of an individual business in accordance with its risk-based approach (RBA). Further, name screening software also provides allied AML compliance solutions such as KYC, CDD, and Transaction Monitoring, which can be integrated according to requirements with the screening software.

Some software also provides the option of integrating screening software with other POS, ERP, and CRM software to help businesses have a one-stop solution.





4. Accuracy

The degree of accuracy in name screening results derived by using name screening software is tremendous as room for human error gets instantly mitigated. Further, this accuracy helps avoid false results, leading to timely implementation of freezing measures and compliance with reporting requirements on the goAML portal.





5. Relying on fuzzy matching algorithms

Fuzzy matching algorithms aid businesses in achieving accurate screening results by removing confusion arising from language variation and phonetic differences. Fuzzy matching features in name screening software help get better results by allowing businesses to alter match percentages according to their screening policy.





6. Audit and procedural recordkeeping

Name screening software helps businesses by creating a record of screenings carried out and ongoing screenings that are continuously monitored, which helps build documentary records necessary for audits and record-keeping requirements.






7. Instant Alerts on matches

Name screening software has a feature of sending immediate notifications to businesses over emails whenever there is a match found while conducting ongoing monitoring or ongoing screening of customers, suppliers or business partners, resulting in the ability of businesses to apply enhanced due diligence mechanisms and fulfilling freezing and record-keeping requirements in a timely manner.



A large, stylized arrow graphic on the left side of the page, composed of three overlapping purple shapes pointing to the right.

TYPES OF WATCHLISTS USED FOR NAME SCREENING

A name-screening exercise will only be as successful and accurate as the selection of appropriate watchlists that help in achieving regulatory compliance applicable to the business.

There are various types of watchlists used to carry out name screening, which are released by international and national authorities overseeing the AML framework.



Some of these watchlists are discussed here as follows:

Watchlists for AML/CFT and CPF Compliance

- ▶ UNSC consolidated list
- ▶ The European Union list
- ▶ The UK HM Treasury list,
- ▶ The United States of America's Office of Foreign Assets Control (OFAC) list
 - OFAC Specially Designated Nationals (SDN)
 - OFAC Sanctioned Countries, including Major Cities and Ports
- ▶ Sanctions and TFS lists
 - Bank of England Sanctions List
 - Canadian Sanctions List (OSFI)





Some of these watchlists are discussed here as follows:

Private Blacklist and Whitelist

- ▶ Businesses can create their own list of individuals they do not want to carry out business with, known as a blacklist and,
- ▶ Create a whitelist, basically containing names of individuals, suppliers or business partners whose names would not generate flags because those are known to the business and have already gone through KYC.





Other Watchlists:

- ▶ Watchlists that provide lists of Politically Exposed Persons (PEPs)
- ▶ Watchlists for detecting individuals and organisations involved in fraud, corruption and bribery
- ▶ Internal and Global Watchlists and databases maintained by Interpol and many other government agencies-issued watchlists such as the FBI most wanted terrorist lists.
- ▶ Media Sources and Database
- ▶ Publicly available Court Orders






Sanctions Screening APIs

API stands for Application Programming Interface that enables other computer programs or software to communicate with one another.

The use of Sanctions Screening APIs, to a great extent, simplify the process of the watchlist screening process. Simply put, sanctions screening APIs can be integrated with the existing POS, ERP, and CRM systems, and the benefits of having a unified compliance software can be availed.



A large, stylized purple arrow graphic pointing to the right, composed of several overlapping, semi-transparent layers of varying shades of purple.

IMPORTANCE OF NAME SCREENING SOFTWARE

Name Screening software gives immediate alerts of matches across ongoing screenings, leading to timely implementation of freezing or transaction suspension measures for compliance with freezing and reporting requirements.

Name Screening Software is important due to its inherent nature of being updated on a real-time basis when it comes to additions, deletions and modifications carried out by regulators in their respective watchlists across the globe.



Name screening software helps get more accurate screening results compared to manual screening, leading to ease of conducting screening. Its fuzzy matching feature considers language, spelling and aliases while generating results.

The automated batch screening feature helps businesses to scale and carry out their bulk screening requirements in the background while issuing notifications or alerts on prompt detection of sanctioned individuals or entities.






What if you do not use Name Screening Software?

Non-compliance with screening requirements, whether intentional or unintentional, when caused by human error of missing out a name or mistake in name screening, be it sanctions, PEP, adverse media or any other watchlists, leads to fines and penalties, damage to the reputation of the business, loss of trust in the business, bans or restrictions getting imposed on the business for carrying out certain or all business activities and even imprisonment in severe cases.

The use of name screening software helps to mitigate the occurrence of human errors, whether intentional or unintentional, increasing the chances of businesses remaining compliant with screening requirements.



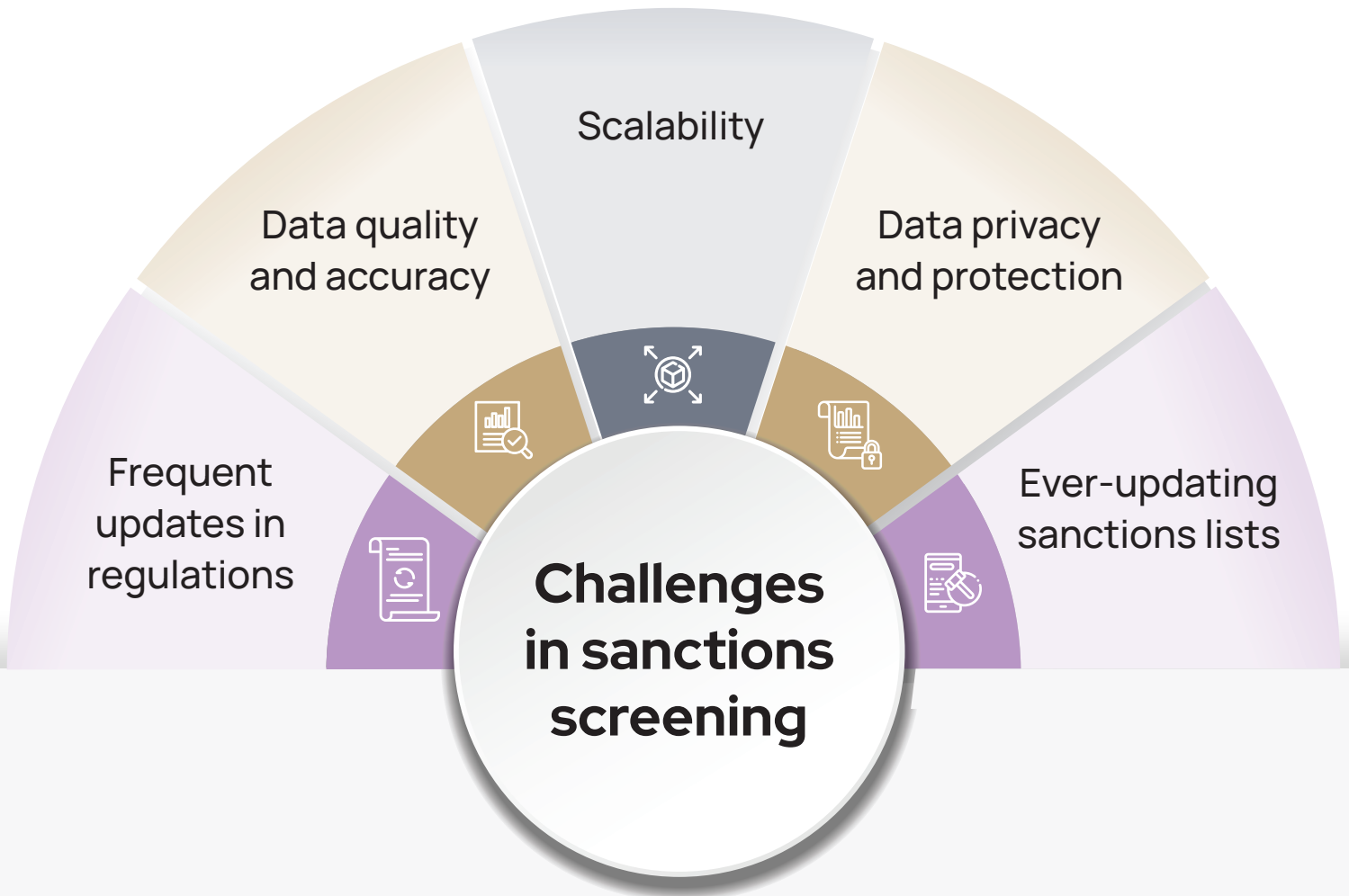
A large, stylized arrow graphic on the left side of the page, composed of several parallel purple lines of varying shades, pointing towards the right.

Challenges in Sanctions Screening

Sanction screening is crucial to ensure compliance with regulations. However, because of its complex, expanded, and time-consuming nature, businesses come across various challenges. It is essential that businesses understand what these challenges are and further take action to address them.



Here is the list of common challenges that a business faces in employing sanctions screening:





1. Frequent updates in regulations

The regulatory landscape is ever-evolving. It's important to stay updated with regulatory changes to avoid noncompliance, which can lead to fines and penalties. Policies, procedures, systems, and controls must be updated and modified to ensure continuous compliance with TFS requirements.





2. Data quality and accuracy

Implementation of an effective sanction screening process is only possible when the database used for screening is updated and accurate, language variations are considered, and discrepancies are removed to eliminate the possibility of errors.





3. Scalability

Initial implementation of a suitable sanction screening process is usually accurately achieved. However, issues arise with the flexibility of the sanctions screening program as business volume increases beyond the scope of the existing sanctions screening system, which results in difficulty in handling large volumes of customer data across multiple sanctions lists.





4. Data privacy and protection

It is important to conduct sanctions screening to fulfil regulatory compliance requirements, but businesses must be mindful that their data privacy notice, which is publicly available, mentions that they use identifiers of their customers, suppliers and business partners key identifier information for carrying out sanctions screening, failing which could result in non-compliance with data privacy and protection laws such as:

- ▶ The Personal Data Protection Law, UAE, Federal Decree-Law No. 45 of 2021, regarding the Protection of Personal Data.
- ▶ General Data Protection Regulation (EU GDPR).






5. Ever-updating sanctions lists

The sanctions lists, PEP lists and other watchlists are updated on a real-time basis by the regulatory authorities responsible for issuing them. However, the challenge arises when businesses are unable to keep up with updated sanctions lists. If they carry out screening across lists that are outdated, the results of such screening would not be accurate. Businesses must be mindful of keeping their database updated to ensure compliance.



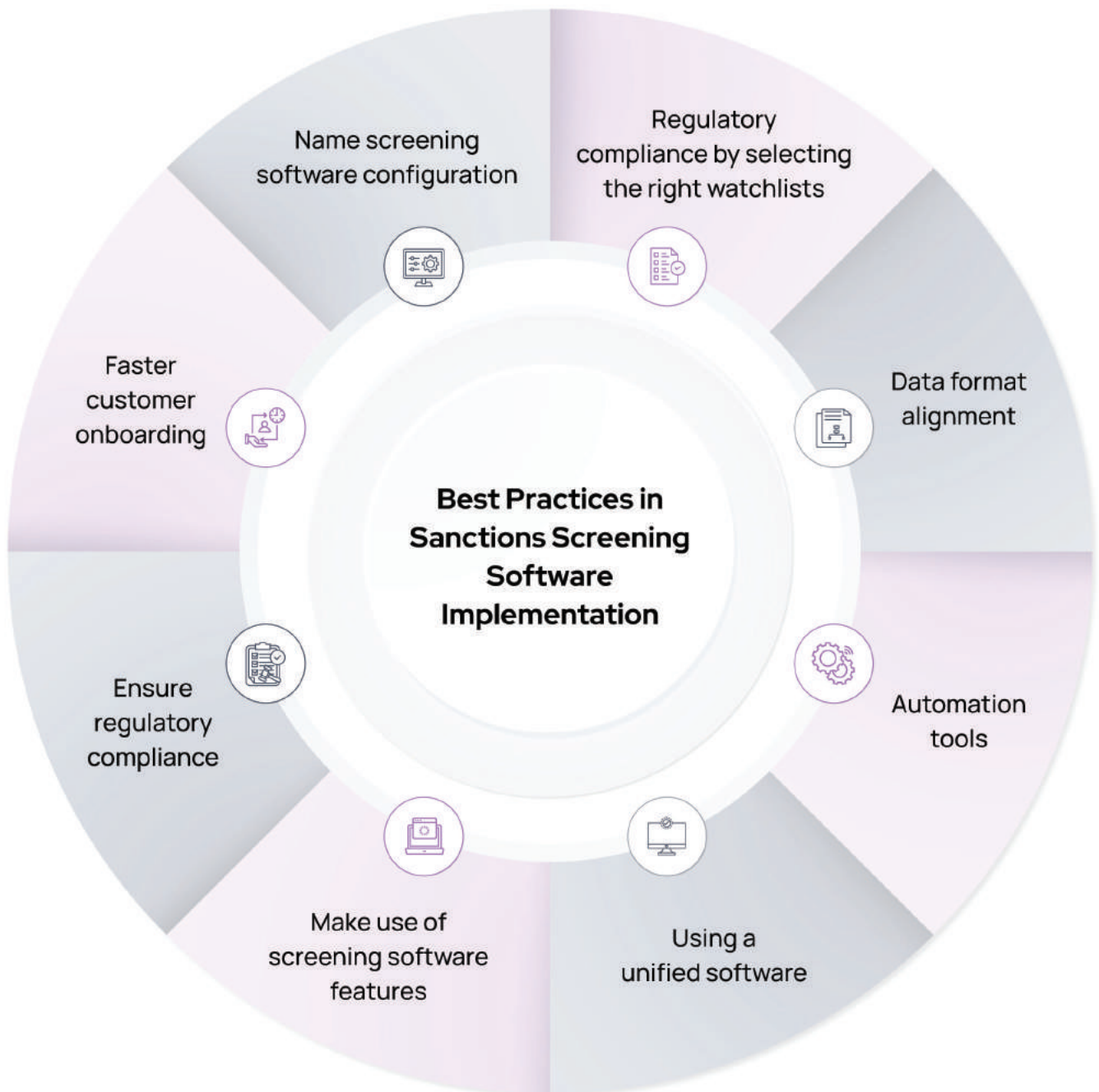
A large, stylized arrow graphic on the left side of the page, composed of several overlapping, semi-transparent purple bands pointing to the right.

BEST PRACTICES IN SANCTIONS SCREENING SOFTWARE IMPLEMENTATION

Businesses require effective sanctions screening to avoid financial damage and ensure compliance with regulations. To implement such effective measures, it is essential to employ software tailored towards sanctions screening. However, when selecting software, businesses should be mindful of certain best practices.



The following is the list of the best practices that a business should consider when implementing sanctions screening software:





1. Regulatory compliance by selecting the right watchlists

Make sure to select, subscribe, and run name screening against all relevant and applicable sanctions watchlists; sanction screening software will help to screen across multiple lists in one go.





2. Data format alignment

Businesses need to be mindful of aligning or arranging their database of customers, suppliers, and business partners according to the requirements of sanctions screening software and screening lists within, particularly when batch screening needs to be carried out, to reduce inaccurate results from screening.





3. Automation tools

While using sanctions screening software, businesses should aim to use automation tools to conduct ongoing screening for bulk screening to avoid manually running single scans. Artificial intelligence and machine learning algorithms can be used to go through a large bulk of databases to save time and ensure accuracy.





4. Using a unified software

Businesses should focus on finding software that helps them fulfil all their AML/CFT and CPF compliance needs of name screening (sanctions, PEP, Adverse Media, etc.) in one software. Businesses may also consider relying on software that has integrated KYC and CDD conducting features to avoid complications and confusion arising out of using more than one platform.





5. Make use of screening software features

Making use of software features such as bulk screening, ongoing monitoring of existing customers, suppliers and business partners, creation of whitelists and blacklists, setting fuzzy match percentages etc., to optimise the use of the software.





6. Ensure regulatory compliance

Businesses can try to ensure that screening software provides the sanctions list needed by the business to ensure compliance with the laws of the jurisdictions in which it operates.





7. Faster customer onboarding

When businesses use comprehensive software that carries out multiple AML/CFT and CPF tasks such as KYC, CDD, and Name Screening, the process and timeline of the customer onboarding cycle reduce drastically, enabling businesses to increase their turnover.





8. Name screening software configuration

Name-screening software enables businesses to configure and set up name-matching rules, where every match identified by the software has a match percentage score associated with it. Based on the closeness of the match, the matching rule will give out the match score.



A large, stylized arrow graphic on the left side of the page, composed of three parallel purple lines of varying shades pointing to the right.

CONCLUSION

Name screening is an indispensable requirement of AML, CFT, and CPF compliance. It forms part of the Customer Due Diligence procedure set out for the business based on the risk assessment carried out for it.

The name-screening process, when carried out by using software or an API, elevates the AML compliance of an organization in several ways as it makes way for customization and integration of name-screening software to suit the individual needs of an organization accurately.



Name screening software and API provide tailor-made name screening services where the organisation can decide which screening lists it needs to subscribe to and whether name screening should include PEP detection and adverse media search for names screened.

Further, the key takeaway of name screening software is its versatility in aiding organizations in complying with their regulatory obligations by generating reports using automation and still involving human intervention while ultimately deriving the final screening report.

This helps ensure that screening analysts, compliance officers, or any personnel of similar skill, competence, or authority can review, assess, and generate conclusive reports using name-screening software.

Below is an example of such an interplay between name screening software and the role of human input in generating the final name screening reports.





Illustrative Name Screening Batch Report

Software Generated Outcome				Human Input and Evaluation		
Sr. No.	Customer Name	Watchlist Name	Screening Result	Result Evaluation/ Review	Review/ Evaluation done by:	Conclusive Screening Finding
1	Chris Ronaldo	Cristiano Ronaldo	Positive	Only the Surname Matches with the customer's surname, and the First Name Partial Matches.	Screening Analyst	Partial Name Match (File PNMR)
2	Taylor Swift	Taylor Smith	Positive	Only the first name matches, and considering the date of birth and other available data points, it's a different person. (cross-verified with KYC documents)	Screening Analyst	False Match (Continue business)
3	Harry Porter	Harry Potter	Positive	Spelling variation (Same person, cross-verified with KYC documents)	Screening Analyst	Positive Match (File FFR)



FAQs

Question -1

Answer:

What is a name screening tool?

Name screening is an essential practice that ensures compliance with AML, CFT, and CPF regulations by comparing names of potential and existing customers, suppliers and business partners against databases and watchlists. Name screening tool is usually a software or an API that carries out name screening using automated systems supported by AI and ML.

**Question -2****What is an example of name screening?****Answer:**

An example of name screening refers to searching the names of natural/legal persons in databases, watch lists, sanctions lists, PEP lists, most wanted criminal lists, etc.

Question -3**What are screening tools used for?****Answer:**

Screening tools are used to identify individuals and businesses included in any of the sanctions lists, watch lists, PEP lists, most wanted criminal list to carry out necessary regulatory compliances such as applying freezing measures, reporting transactions to the FIU through the goAML portal.

Question -4**How to do AML screening?****Answer:**

AML screening can be carried out by collecting key identifier details of natural and legal persons, such as full name and date of birth, entering such details into screening software, and checking results to ascertain whether a match is confirmed against any of the names in watchlists or no match is found.



Question -5

What is fuzzy logic name screening?

Answer:

Fuzzy logic is a method that simplifies screening processes by taking into consideration the extent of accuracy. In the context of name screening, fuzzy logic is relied upon to factor in phonetic, script, pronunciation, spelling variations, and other differences in names and errors.

Question -6

How do you screen PEPs?

Answer:

PEP can be screened by entering details as follows:

- ▶ Full name/ Script Name (Cyrillic, Arabic, Russian, etc.)
- ▶ Date of birth or year of birth
- ▶ Country of political exposure
- ▶ Gender
- ▶ Politically exposed role and responsibility
- ▶ Appointment date

and checking the screening result to find out if any match is found or not.





Question -7

What is AML sanctions screening?

Answer:

AML sanctions screening is a process where names are scanned against sanctions lists issued by various authorities to break the chain of financial crimes by detecting and preventing the entry of criminals into legitimate financial systems. Sanctions screening prohibits business with certain individuals, entities, groups, industries, and countries, to name a few.

Question -8

How are screening tools selected?

Answer:

Factors to be considered by businesses before selecting a screening tool are as follows:

- ▶ Assessing risks faced by it, i.e., the risk-based approach to identify risks, it is vulnerable to and assess which screening lists it needs to subscribe to;
- ▶ Understanding its need and creating a list of must-haves that are non-negotiable;
- ▶ Shortlisting screening tools and going through demos to assess technical adequacy;
- ▶ Cost-benefit analysis;
- ▶ Screening tool purchase decision.



**Question -9****How is screening different from assessment tools?****Answer:**

Screening generally leads to a result that is either:

- ▶ Positive
- ▶ Negative
- ▶ Inconclusive

However, assessment tools give results diagnostic and elaborate results that cannot be categorised distinctly as results differ from case to case, considering factors such as missing data, recommendations of enhanced due diligence etc.

Question -10**Is name screening a sanction control?****Answer:**

Name screening covers various types of screening processes under its umbrella, such as sanctions screening, PEP screening and Adverse media checks.



**Question -11****Is screening part of the KYC and CDD process?****Answer:**

Screening is a part of KYC as it helps businesses to reduce the incidences of financial crime such as ML, FT and PF by screening such customers against sanctions, PEP and various AML-related watchlists to prevent them from entering the economy.

Question -12**Why is screening important in the AML KYC and CDD process?****Answer:**

Screening is important because it ensures:

- ▶ Effective customer monitoring
- ▶ Identification of high-risk customers



**Question -13****What are PEPs and sanction screening?****Answer:**

PEPs and sanctions screening are part of AML compliance, requiring the identification of politically exposed persons and, sanctioned legal entities and natural individuals and screening them against the sanction list to comply with legal obligations.

Question -14**How do you conduct a PEP screening?****Answer:**

PEP screening is conducted by using the following steps:

- ▶ Using reliable and updated PEP definitions and databases
- ▶ Keeping secondary identifiers ready to eliminate false positive matches.
- ▶ Staying updated with the latest regulations
- ▶ Screen connected, related individuals such as family and associates



**Question -15****What is screening in AML KYC?****Answer:**

Screening in AML KYC includes screening potential and existing customers across various AML checklists to prevent conducting business with individuals and entities named in the watchlists.

Question -16**What are the types of screening in AML?****Answer:**

Common screening types in AML are:

- ▶ Sanctions and TFS screening;
- ▶ PEP screening;
- ▶ Adverse media screening;
- ▶ Anti-corruption and anti-bribery screening;
- ▶ Related watchlist screening



**Question -17****How to do screening in the KYC and CDD process?****Answer:**

Screening during KYC involves collecting customer information, verifying their identity and scanning them against the relevant sanctions list.

Question -18**What is the difference between monitoring and screening in AML?****Answer:**

Monitoring is an ongoing process where business relationships are monitored during the course of business, and screening is matching names of customers across lists issued by regulators.

Question -19**What is the screening process in banking?****Answer:**

The practice of collecting and verifying customer information, such as name, date of birth, address, and other relevant details, and cross-referencing it against various watchlists, sanctions lists, and relevant databases.



ABOUT RapidAML

RapidAML is an AML software designed to support the compliance tasks of the DNFBPs and the VASPs, offering an advanced and secured technology platform



Who we are

Facctum, founded in 2021 by a group of enthusiasts who have experience in banking, financial crime risk management technology, data science, etc., specialises in building risk management solutions with new-age technology.





Our Mission

We understand the significance of AML compliance and recognise its complexity. Addressing this issue is our mission at RapidAML.

Our solution focuses on simplifying the intricate regime of AML compliance with advanced technology. We aim to help the regulated entities, specifically the DNFBPs and the VASPs, smoothen their AML efforts with RapidAML's end-to-end AML software.





Our Vision

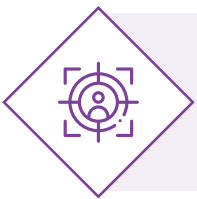
Our vision is to develop next-gen AML software that offers an affordable and complete solution to all the AML compliance-related issues of every DNFBP and VASP worldwide.





Our Core Values

We live by these guiding principles that guide our progress



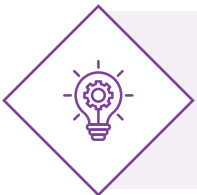
Customer Focused

We are committed to offering quality AML support to exhibit a constructive effect on the customer's business



Elevated Excellence

With a comprehensive, tech-driven financial crime compliance solution, we nurture customer's efforts and ignite brilliance to AML function.



Innovation Is The Key

We strive for healthy competition, bringing out the best version of the AML tools and technologies with continuous research and improvement.



Integrity

We value our customers, our team, and our society, and we build trust with our committed honesty and transparency.



Together We Win

With inclusiveness and a sense of collaboration, we assist our customers in accomplishing compliance and developing a sense of shared achievement.



RapidAML

 www.rapidaml.com

 info@rapidaml.com

