Guide on use of automated systems for the prevention of money laundering and terrorist financing

Monitoring & Compliance | February 2024 | Guidance

CONTENTS

1. INTRODUCTION

This guidance has been prepared by the Compliance Committee of ICPAC and it endeavours to provide some insight on how to assess automated solutions specializing in the prevention and suppression of money laundering and terrorist financing. The current guidance paper replaces the previous guidance paper issued on 25/7/2016 'General Circular 14/2016 (GE_14/2016): Systems for the prevention of money laundering and terrorist financing'.

The purpose of this paper is to assist obliged entities in selecting the most appropriate AML/CFT software solution that will support the work of the compliance department of the firm in fulfilling its obligations whilst at the same time enhance efficiency and productivity levels.

2. ANTI-MONEY LAUNDERING SOFTWARE SOLUTIONS

An anti-money laundering software comprises of a variety of technologies designed to prevent, detect, and report potential money laundering activities and related financial crimes. It is frequently used by regulated organisations to assist in compliance with AML and countering financing of terrorism (CFT) regulations.

AML software often includes features such as:

- risk profiling
- ID verification
- customer due diligence (CDD)
- watchlist/background screening
- transaction screening and monitoring, reporting,
- and may have embedded audit trail capabilities

It's important to note that AML software is not one-size fits-all and should be tailored to the specific needs and risks faced by each organization taking into account the size and type of the portfolio of clients held, as well as the type of services offered by the firm.

The automated nature of such systems allows the firm's policies and procedures to be applied faster, more efficiently and targeted at cases through the introduction of rules, validations, alerts and report generation.

3. ASSESSMENT AND EVALUATION OF SOFTWARE SOLUTIONS

It is the responsibility of the Compliance Officer to assess the appropriateness of a system for its firm and ensure that it is set up, maintained and updated periodically and/or when the need arises.

A **non-exhaustive list** of factors that should be considered as part of this assessment and evaluation is provided below, providing guidance to Members in making an informed decision for their organisation's AML software needs. Note that this is indicative and additional factors may need to be considered based on specific circumstances.

3.1 Evaluating the provider

As part of the vendor assessment, the below factors should be considered amongst others:

- **Expertise** to develop, upgrade and maintain the system. To assess the knowledge of the subject matter and experience in the field, review the vendor's website, look through brochures, number of years in the field, client references, CV and qualifications, memberships held with relevant professional bodies or industry associations, other forms of external recognition, awards accredited, published papers or books written by the vendor)
- **Relevance** of vendor to AML related systems. Check the vendor's profile including other types of services provided, other systems developed and key areas of expertise in which the vendor is investing.
- **Reputation**: background checks, references from third parties, clientele base and important projects undertaken, website information, participation in AML events. Consider also anti-bribery and anti-corruption procedures in place by the vendor.
- **Capabilities**: geographical location, proximity to vendor and ease of access, time, and resources available, engaged team sufficiently trained and in a position to provide continuous support, upgrades and quality services.

- **Conflicts of Interest and Independence** checks should be performed, for example consider how this provider was referred to your firm.
- **Financial soundness** of vendor: for the development, updating and maintenance of the AML tools and provision of ongoing support required. Also ensure that the vendor has adequate liability coverage.
- **After sales training and support**: supportive services including ongoing training, technical support and maintenance by the vendor's team. Business continuity plan to be considered if in place.
- **Dynamic team:** publication of relevant guidance**,** webinars, physical seminars, online you tube video demos, user manuals, circulars and guidance, presentation of changes and updates made to the system etc.
- **Dynamic system:** frequent updates and system enhancements is a strong indicator that the vendor is keeping ahead of technological developments.
- **Cooperation with other providers** (subcontractors) – It is important to establish any relationships with other subcontractors and evaluate them as a whole.
- **Disaster recovery plan:** ensure the provider has a response plan in cases of unplanned incidents or disasters that could significantly disrupt its regular business operations.
- **Data protection and information security**: Ensure that the vendor is aware of the GDPR requirements and is in a position to demonstrate compliance. Also, it must be ensured that the information security framework of the vendor is strong. Some factors to consider may include for example:
    - Use of Encrypted connections/databases
    - Recognition of terminated clients and automatic deletion of personal data in accordance with the AML laws
    - Data anonymization option (e.g. for terminated clients)
    - Transfers of Data outside EU
    - Use of subcontractors
    - User access rights, restrictions, password protection
    - User log keeping an audit trail
    - Data Security Certification (e.g. ISO 27001)

- Data Protections Impact Assessment (DPIA)
- Consider previous data breaches, if any to be disclosed by the provider.
- Relevant work on GDPR systems
- Participation in GDPR events, projects
- Request results of latest Data Protection Impact Assessment or perform penetration testing to identify vulnerabilities.

It is also recommended that members sign confidentiality and data processing agreements with the provider.

3.2 Evaluating The AML System

Assess whether the system provides a **complete AML solution** for your Firm. Some of the relevant tools and features you could consider are outlined below:

3.2.1 "Customer database– Know Your Client"

This is the basic module that should allow the users to record data on the profile of their clients (legal and natural persons) including basic contact details and identification information as well as geographical data and financial data amongst other. Information imported could relate to the client's legal entity, its shareholders, beneficial owners (BO), directors as well as other counterparties relevant to the KYC process. The AML solution should have the ability to automatically create records for the legal entity, each shareholder and each BO and associate them with the entity records, improving productivity and reducing manual effort. It should also have the capacity to connect persons and entities between them and offer a diagrammatic depiction of the relationships identified (e.g. shareholding structure or group structure).

Furthermore, as part of the KYC process, supporting documentary evidence is maintained in electronic format within the system itself, as an option. Document management and record-keeping features in the AML software prove to be useful in complying with record retention requirements supporting the client identity verification process performed. Also refer to section 5 below.

Additional features to look for:

- ✓ The system could have the added capacity of **notifying** the user when identification documents are close to expiry e.g. passports, IDs etc. This again acts as an embedded control feature and assists the compliance officer in monitoring compliance.
- ✓ The system could also notify the user when the KYC process needs to be reperformed, that is based on the cycles defined in accordance with the risk assigned to each client.

3.2.2 "Risk Assessment tool"

Further to the basic KYC process, the AML system is capable of performing a risk evaluation of the client based on the information collected and recorded through the system. The AML system should be fully aligned with the requirements set down by the AML Law and Directives based on which the risk evaluation is performed.

The compliance solution should be able to assign risk scores to customers and entities based on predefined risk factors such as customer type, geographical location, sanctioned and PEP screening results, product/service type and other factors. For further guidance on the risk assessment requirements, please refer to GC 6/2019: Guidance paper on the Risk Based Approach (RBA), last updated in May 2022.

A crucial aspect of the AML software is its ability to recognized higher-risk characteristics that would result in a high-risk client profile overall, such as PEP status or links to high risk third countries (as strictly provided for in the Cyprus AML Law) as well as other cases presenting high risk of money laundering and terrorist financing in accordance with the risk appetite of the user. This empowers organizations to proactively identify and mitigate potential AML risks in a timely manner.

In addition to the above feature, the AML software may have the ability to tailor the client due diligence process in accordance with the resulting risk score assigned to each client ensuring that enhanced due diligence procedures are performed for higher risk clients and simplified due diligence procedures for lower risk clients.

Additional features to look for:

- ✓ Some **risk factors that are dynamic** and need to be updated on a continuous basis, such as geographical risks attached to jurisdictions based on the lists published by the European commission, the FATF, EU tax lists and other. The compliance officer should ensure that the system immediately reflects any changes to country risks or client risks (e.g. PEP status-see below) so that customers impacted are re-evaluated promptly. Some systems have the capacity of alerting users of any changes made to risk factors and notify the user regarding customers that require re-evaluation, as an additional embedded control feature. The compliance officer should look for such embedded control features which assist in compliance with the AML law and provide comfort in compliance.
- ✓ **Client retention**: In the meantime, if there are no changes impacting the assigned client risk levels, the system could still notify the user when the risk evaluation process needs to be reperformed, that is based on the cycles defined in accordance with the risk assigned to each client.

3.2.3 "Client screening tool"

The tools usually provides the option of client screening. The tool will conduct a background screening check on the full name (and date of birth and other parameters for more precise findings) of the client (natural person, client entity, vessel, aircraft) through specific databases to determine whether the client is linked to unfavourable information, negative publicity, litigation court cases, or sanctions and restrictive measures. The tool will also return any true match against PEPs (Politically Exposed Persons) and immediate family or close business associates (Level 1, 2 and 3) as well as Sanctions Designated Persons.

The AML solution should be capable of screening not only customer and entity names, but also counterparties identified within underlying agreements/transactions, recipients of funds/ beneficiaries, authorized signatories, nominees, trustees and others on a risk-based approach.

Additional features to look for:

- ✓ **Sanctions**: The compliance officer of each firm should assess the sources used by each vendor in order to conduct screening checks. The tool should cover as a minimum, lists with **Politically Exposed Persons (PEPs), EU restrictive measures and UN sanctions, OFAC for US sanctions, OFCI for UK sanctions.**
- ✓ **PEP Level**: The compliance officer should ensure that the system clearly defines the PEP level when returning a 'true match' report, that is usually PEP Level 1, 2 or 3. The compliance officer should have a good understanding of each level and risk involved.
- ✓ **Resources**: The compliance officer needs to obtain a basic understanding of the system and the resources it uses as well as the true matches it will report to the user. Specifically, some databases may not incorporate information that is not yet validated, such as negative publicity, allegations and other information that has not been ascertained. Other databases/lists may also include adverse information other than the restrictive measures. The compliance officer should carefully assess the needs of the firm in deciding which tool best fits the firm's needs.
- ✓ **Integration**: The compliance offices should check what integration the screening tool provides and ensure that in case the firm may decide to switch to another tool, this can easily be done.
- ✓ **Ongoing monitoring and batch checks**: The opportunity is provided for regular (even daily) mass comparison of clients against lists. The types of lists and the indicative databases are mentioned above. The systems provider should ensure and be able to demonstrate the continuous updating of the lists. A daily mass check of the clientele is recommended in order to ensure that any matches against the clientele are identified immediately. This option should be provided further to the ad hoc option that is necessary.

3.2.4 "**Transaction monitoring tool**"

Provides the ability to include predefined scenarios, create rules or algorithms that analyse transaction data for patterns or anomalies that would trigger red flags as part of transaction monitoring process. The standardised rules usually included in the systems must be tested by the compliance officer of each firm and the system should have the capacity of allowing for any

modifications to the level and type of monitoring based on the customer's risk profile, the organisation's risk appetite, compliance management, as *well as local regulatory requirements.*

Additional features to look for:

- ✓ Some tools use machine learning and Artificial Intelligence which enhances the transaction monitoring and makes it much more efficient and effective for the compliance team. **The compliance offices should assess the solution provided and its ability to evolve as well as its flexibility and agility in this fast-changing technological environment.**

3.2.5 "Record keeping and Data Protection"

The AML system should be able to support organisations in meeting requirements with respect to record keeping, document storage, and on maintaining an adequate audit trail. The user should be provided with the option of retaining records of customer identification and verification documents collected during the customer due diligence (CDD) process, such as copies of identification documents, transaction records, and other relevant information within the system.

Furthermore, the software solution may assist the user in maintaining a comprehensive audit trail that captures all actions performed on client records, serving as evidence of due diligence efforts in the event of a regulatory visit by the competent authorities or for the purpose of internal audits undertaken within the organisation.

In accordance with the provisions of the applicable data protection legal and regulatory framework, including Regulation (EU) 2016/679 (General Protection Regulation) **("the GDPR")** and the Personal Data Law, organisations need to ensure that they maintain secure storage and implement robust access controls for AML records and documents to ensure data integrity, data security and confidentiality. The AML solution provider should be able to accommodate such requirements as covered within section 3.1. above.

3.3 Other Parameters

In addition to the solutions available in every system there are other parameters that must be taken into account as follows:

- Whether the system has been developed by the same provider or whether the provider is acting as an intermediary
- Whether there is direct access to the manufacturer
- How flexible and transparent the system is, i.e. can the user modify the embedded risk factors, risk criteria, answers to given risk criteria, weight factors assigned to each risk factor, resulting risk level generated by the system and so on. ***It is important to note that the risk factors as well as the risk weights attached to each risk factor by the system needs to be reviewed and approved by the Compliance Officer. The compliance officer should be able to review and modify the risk assessment to align this fully with the firm's AML program and underlying risk assessment methodology. The compliance officer bears the ultimate responsibility of ensuring that the risk assessment is in line with the requirements set down by the AML Laws.***
- How user friendly it is: the AML tool should be easily understood and applied by members of staff at different departments and from different levels.
- Does it allow multiple users and various access rights (e.g. administrator, user, auditor, Compliance Officer etc).
- How fast it responds to the fast-changing technological environment as well as to the underlying AML laws and regulations.
- Whether it maintains a "history log" and an "audit trail": The history should record client risk assessments performed, reasons for re-evaluations and changes implemented and dates of such changes/updates made, history of client screenings performed, amongst others. The history log should assist the compliance officer in demonstrating compliance in case of an external monitoring or regulatory visit.

  Production of dynamic reporting: Whether the system provides valuable reports based on the information included which assist the compliance officer by providing live client data and statistics and also would assist in preparation for the various reports required by then

regulators e.g. Annual AML questionnaire and client statistics and information for ASPs. Having a **centralized system** for all AML requirements including compliance reporting, performance of firm wide risk assessments and sanctions risk assessments would also be beneficial to the compliance team.

The Institute emphasizes that it is the responsibility of the Firms to carry out a thorough evaluation of third party providers and their systems and document the process prior to subscription to these, taking into account all of the above factors and to proceed with the cooperation only after ensuring that the system meets the basic provisions of the regulatory framework with respect to KYC and due diligence requirements, risk assessment process, client retention procedures and background screening checks.