Effective screening controls for sanctions and AML risk management
Recent record fines for sanctions breaches and failure to identify Politically Exposed Persons (PEPs) have led to closer scrutiny of screening controls. But rather than effectively mitigating the risks, a common approach is simply to drop thresholds and augment the workforce. While these actions may be required to some extent, a more measured approach will help to control costs while also addressing gaps in existing controls.

Screening programs continue to follow industry trends – often mistaken to be “best practice” – rather than fully understanding the risks and responding with a proportionate control framework. Such a framework is likely to be achieved by instead cutting watch-lists and focusing on areas of risk previously overlooked.

“Over-screening” is prevalent, with watch-lists including targets from distant sanctions regimes and “PEPs” who are not really PEPs at all. Meanwhile, financial institutions (FIs) tend not to screen domestic transactions due to a tacit agreement across the industry to rely upon each other’s customer screening controls. And, although systems are in place to monitor the money laundering risk associated with transactional behavior, no such controls are in place to evaluate the money laundering risk of transactions from the perspective of who they involve.

An advanced sanctions prevention and Anti-Money Laundering (AML) screening program would consider:

1. **Tailoring the content and application of watch-lists to the organization’s risk profile and appetite** – significant operational cost savings can be made by streamlining watch lists in the following ways:
   - Identifying a “core” set of sanctions lists to use for all customer relationships and transactions, and only utilizing lists belonging to other regimes where particular scenarios (e.g., destination of a transaction) dictate that this is necessary
   - Determining the organization’s definition of a PEP upfront (e.g., based on public office held, country of office, relationship with the primary PEP, etc.) and tailoring PEP lists accordingly
   - Avoiding duplication across screening controls – e.g., FIs may determine that it is not necessary to re-screen their own customers in transactions when they have already been screened against the relevant lists

2. **Screening unconventional but known areas of sanctions and money laundering risk** – real risks are present in some previously overlooked areas:
   - In domestic transactions involving sanctions targets – relying on the customer screening controls of other domestic institutions could lead to a breach occurring
   - Where individuals and organizations that pose a high risk of money laundering (e.g., PEPs) are transacting with the organization’s customers; it is likely many transactions involving such targets should give rise to suspicion of money laundering activity
There is no obligation to screen customers or transactions. It is recommended by the Joint Money Laundering Steering Group (JMLSG)\(^1\) as a practical method for identifying sanctions targets but it is a means, not an end. FIs must be careful that they do not lose sight of the objectives they are attempting to meet with their screening program. There are at least four objectives which screening may be used to help address:

1. **Sanctions**: To not permit financial transactions with sanctions targets
2. **Enhanced Due Diligence (EDD)**: To undertake EDD on PEPs and other high risk customers
3. **Suspicious activity**: To identify suspicious activity that may be indicative of money laundering
4. **Negative news**: To undertake negative news searches as a part of EDD on PEPs and high-risk customers

The disparate range of objectives may, in itself, shed some light on the sometimes conflicting priorities in screening programs. For each objective, there is a need to accurately identify an individual or organization (a “target”) in order that some other action can be taken, whether it be stopping a transaction or identifying the need to undertake additional due diligence. It may be argued that the “Suspicious Activity” objective is more relevant to an AML transaction monitoring program than a screening program. However, its relevance here is in relation to the fact that transactions can be suspicious in virtue of the counterparties they involve, not just the behavior which they exhibit.

Most screening programs implement at least two main screening controls to help meet these objectives: customer screening and transaction screening. Customer screening is used to identify new or existing customer relationships which may involve targets of interest; transaction screening is used to identify transactions involving such targets. Together, customer and transaction screening are intended to form a complete set of automated\(^2\) screening controls for identifying sanctions, PEPs and other high risk targets entering the organization or having financial dealings with it. However, there are a number of limitations in the way in which these controls are implemented, often resulting in risks not being effectively managed and significant inefficiencies being introduced into the screening programs.

---

\(^1\)JMLSG Part III 4.32-4.60 (Note: As stated by JMLSG, the guidance in Part III “does not carry the same Ministerial approval as the guidance in Parts I and II.”)

\(^2\)Additional manual controls are often in place – e.g., use of Customer Due Diligence (CDD) processes to identify PEPs
The following diagram represents the interactions a typical FI may have which will expose it to high risk individuals and organizations. These interactions include starting a new customer relationship, continuing an existing customer relationship and transacting with other organizations (including an organization’s own affiliates). It also highlights the points at which customers or transactions may be screened during the different interactions and the types of lists that they may be screened against.

Potential gaps and inefficiencies in screening controls

The diagram shows the interactions and the points at which customers or transactions may be screened. The lists included are Sanctions, AML, and Adverse media. The key indicates the risks associated with each interaction and the types of screening that may occur.
The different points at which screening might be undertaken are enumerated in the following table, along with some observations and potential areas of concern.

<table>
<thead>
<tr>
<th>Title</th>
<th>Observation</th>
<th>Potential gap?</th>
<th>Potential over-screening?</th>
</tr>
</thead>
</table>
| 1 New customers | ► New customers are screened against sanctions and AML lists  
► New customers are only screened against negative news if the customer is high risk | No | Yes:  
► Targets which pose a low risk of money laundering  
► Extraneous sanctions entries |
| 2 Existing customers | ► Existing customers are screened against sanctions and AML (e.g., PEP) lists when either the customer record changes or the list changes (and sometimes also during a periodic review)  
► Existing customers are only screened against negative news if the customer is high risk | No | Yes:  
► Targets which pose a low risk of money laundering  
► Extraneous sanctions entries |
| 3 All transactions (with other organizations, including affiliates) | ► Counterparties are rarely screened against AML lists | Yes:  
► Counterparties which may pose a money laundering risk are not screened | No |
| 4 Domestic transactions (including Single Euro Payments Area [SEPA] transactions in the Eurozone) | ► Counterparties in domestic transactions are not screened against any lists | Yes:  
► In cases where other organizations’ screening controls cannot be trusted, sanctions targets may be missed | No |
| 5 International transactions | ► Originators and beneficiaries (i.e., both customers and counterparties) in international transactions are screened against sanctions lists | No | Yes:  
► Sometimes sanctions lists used are not specific to the jurisdiction(s) involved  
► For transactions between affiliates of the same organization, where the screening controls are known to be equivalent, there is duplication in screening the transaction at both origin and destination  
► Re-screening own customers in transactions |
Sanctions gaps and over-screening

As indicated in the table above, there are a number of potential gaps and cases where screening programs may be “over-screening” – i.e., screening for targets which do not pose a significant risk. A number of these areas relate to sanctions risk specifically, and one such area is domestic transactions. Informal convention has led FIs across the industry to not screen domestic transactions for sanctions targets. This is probably due to the assumption that other FIs within the country will have a similar standard of customer screening controls, and therefore, domestic transactions are unlikely to involve sanctions targets. However, an FI is unlikely to be able to argue that it did not have “reasonable cause to suspect” it was providing financial services to a sanctions target on the grounds that it assumed others were effectively managing the risk. Each FI is individually responsible for this risk. The numerous fines received by FIs for sanctions breaches in recent years are testament to the fact that the controls of others cannot be trusted indiscriminately.

It may be argued that a bank (Bank B) holding an account for a sanctioned individual, is more likely to fall under scrutiny than another domestic bank (Bank A) that processes a transaction to the account held by Bank B. However, both have breached financial sanctions and so both have committed an offence.

\[\text{\textsuperscript{3}Terrorist Asset-Freezing etc. Act 2010 §12-14}\]
Another assumption made is that all cross-border transactions do need to be screened because controls in some countries are weaker. For example, in the diagram above the Bank B would not screen transactions with Bank A but it would screen transactions with Bank C because they are cross-border. However, in many cases there is no reason to believe that the strength of controls is any more varied between banks in different countries than it is between banks within the same country. Indeed, for at least some European countries the level of variation in controls is similar. Therefore, it seems arbitrary to assert that cross-border transactions ought to be screened and domestic transactions should not. There can be challenges in obtaining the relevant data for screening domestic transactions as they often do not have as rich information relating to the originator and beneficiary as wires do. However, given that FIs have sufficient information to carry out these transactions, data quality is unlikely to provide a defense.

Another concern from a sanctions perspective is the amount of over-screening which occurs, particularly when FIs utilize third party list providers for customer screening. Often it is assumed that all sanctions lists should be screened. Though sanctions regimes can be extra-territorial (notably the US regime), they are typically limited by one or more of the following:

- **Jurisdiction** – transactions involving the jurisdiction the regime belongs to
- **Citizenship** – nationals of the jurisdiction the regime belongs to
- **Currency** – transactions in the currency that belongs to the regime
- **Correspondent banking** – existence of correspondent banking relationships with banks which have operations in the jurisdiction the regime belongs to

The fact that regimes are limited means that for any given customer relationship or transaction, many sanctions lists may not be relevant. For example, a primarily European bank may determine that when opening a new customer relationship that screening against a Chinese sanctions list is not relevant even if the potential customer is Chinese, as it may have no obligation to comply with the Chinese sanctions regime.

---

*Sometimes even when the transaction does not involve a jurisdiction, national or currency related to the regime the existence of a correspondent banking relationship can mean financial transactions of any kind with entries on the regime’s list are forbidden.*
If that bank (Bank A) could potentially transact with China then it may need to comply when such transactions occur. In this case, it may decide to implement a complementary transaction screening control so that, when it does transact with China, it does screen the payment – including both its customer and the counterparty – against the Chinese list to help prevent any breaches occurring.

The benefit of taking this approach is that each additional entry on a sanctions list can lead to many more false positives and so only using the list entries required for the given situation can significantly reduce operational cost. The risk appetite of many FIs may dictate that certain “core” lists should always be used for screening (e.g., United Nations (UN), European Union (EU), Office of Foreign Assets Control (OFAC), Her Majesty’s Treasury (HMT)) but, outside of these, there are many other lists which can be used in a more targeted manner.

Many FIs will screen both the originator and beneficiary in transactions, where often one of these will be its own customer which will have already been screened against its “core” lists (at a minimum)\(^5\). In such circumstances, as long as the FI has confidence in its customer screening controls, it could choose to only screen the counterparty in the transaction to avoid duplicating effort. It would only re-screen its own customers when the transactions involve jurisdictions outside of those included in its “core” lists. Organizations with robust screening controls in place may further reduce duplication by choosing not to screen transactions with their own affiliates (or to only screen the transaction once, rather than at both origin and destination) where they know parties on both sides of the transaction have already been screened using customer screening controls.

---

\(^5\)Where an FI is acting as an intermediary, it may be the case that neither the originator or beneficiary are its customers
AML gaps and over-screening

In addition to screening challenges from a sanctions perspective, there are also often a number of gaps from an AML perspective in screening controls. Identifying suspicious activity which may be indicative of money laundering is traditionally seen as falling within the remit of AML transaction monitoring, not screening. However, the involvement of individuals or organizations considered to pose a high risk of corruption, drug trafficking or other criminal activity in transactions could be a key indicator of suspicious behavior. Indeed, many would agree that a transaction involving the leader of a drug cartel is much more likely to be suspicious than a transaction involving a “round amount” (e.g., €10,000). As transaction monitoring systems are not typically designed to identify these targets but rather to identify patterns in transactional behavior, such transactions are often overlooked. Consequently, it seems likely a large proportion of suspicious activity is being missed.

Screening controls are better designed to identify this type of behavior given their name matching capabilities. As with transaction monitoring systems, it is likely these transactions do not need to be screened real-time as in most cases these transactions do not need to be stopped (unless it is known in advance that they will occur). This will avoid overloading the screening systems as this type of screening could be executed during periods of low traffic. Screening counterparties against a tailored list of these high risk targets in this way would significantly increase FIs ability to identify money laundering.

Despite the need to enhance screening controls from an AML perspective, there is often also significant over-screening in this area. Lists utilized for screening new customers or existing customers, especially for larger FIs, are invariably based on commercially available lists. One of the main reasons for this is that such lists are a source of PEPs around the world, which are not readily available on official lists. However, the definition of “PEP” these providers use is so broad that it includes many individuals in different public offices and their associates which would not fall under the definition provided in regulation. This breadth gives flexibility with regard to an FI’s risk appetite but, if not carefully managed, can lead to many individuals being screened which are not of interest to the organization in question.

For example, the aunt of a local mayor in a country with a low risk of corruption is likely to pose a very different risk to a member of the national legislature in a country with a high risk of corruption⁶. If for some reason the aunt in question did have considerable influence over government funds, this information is much more likely to be ascertained through the use of robust CDD procedures than through the use of screening. Given that as much as 75% of commercial lists can be made of these “PEPs”, there is significant opportunity in this area to reduce the size of watch-lists and the operational cost associated with screening them. FIs should consider reducing such lists by identifying which public offices and types of associates they consider of importance for each jurisdiction. Exceptional cases where individuals possess an unusual amount of influence for their role can be managed using CDD instead.

---

⁶Risk of corruption could be identified using the Corruption Perceptions Index, for example
Taking a more measured approach to screening

Given the number of potential gaps that are present in screening programs and the amount of over-screening that occurs, it is clear that better evaluating the risks and tailoring the response accordingly could make screening programs much more effective and efficient. In the future, FIs that enhance their programs in the ways described here will have a significant competitive advantage, from both a risk and a cost management perspective.

How EY can help

EY has significant experience of working with financial institutions of all sizes to assist them with their screening programs. EY can help with:

► Screening controls maturity assessment
► Policy review
► Process review and optimization
► System rules and configuration review
► System testing
► Watch list management and optimization
► Data quality assessment
Effective screening controls for sanctions and AML risk management

Contacts

Hamish Thomas
Partner
EMEIA FSO Advisory, Financial Crime Compliance, Ernst & Young LLP
T: + 44 20 7951 1955
E: hthomas@uk.ey.com

Debbie Ward
Partner
EMEIA FSO Advisory, Financial Crime Compliance, Ernst & Young LLP
T: + 44 20 7951 4622
E: dward1@uk.ey.com

Richard Elliot-Cooke
EMEIA FSO Advisory, Financial Crime Compliance
T: + 44 20 7783 0043
E: relliot-cooke@uk.ey.com

Scott Sarsam
EMEIA FSO Advisory, Financial Crime Compliance
T: + 44 20 7783 0769
E: ssarsam@uk.ey.com
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2016 EYGM Limited.
All Rights Reserved.

EYG No. 01049-164Gbl
1432522.indd (UK) 06/16. Artwork by Creative Services Group Design.
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com