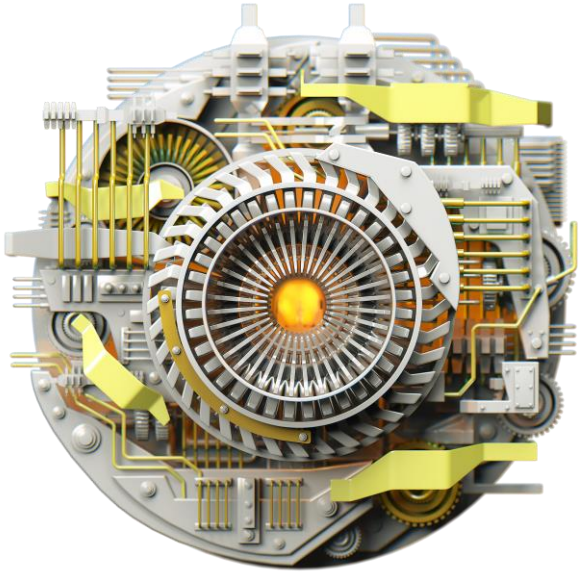
Deloitte.



Data management: Why it matters for effective sanctions screening

1. What is sanctions screening and who performs it?

In 2019, enforcement actions and investigations into sanctions violations has resulted in fines of $10bn for non-compliance with AML, KYC and sanctions regulations.[1] Some notable examples of fines are $8.9bn paid by BNP Paribas in 2014 to the US authorities for breaches of US trade sanctions, in 2020 Standard Chartered Bank was fined US$24.9 million for a serious breach of sanctions by providing around U.S. $119.1 million in loans to a Russian bank in the Ukraine and in 2018 Société Générale agreed to pay US authorities $1.3bn to resolve a case involving the handling of dollar transactions in violation of US sanctions.[2,3] An association with a sanctioned individual, entity or country can also lead to significant reputational damage for a financial institution.

The Wolfsberg Guidance on Sanctions Screening states that financial institutions are required "to maintain an effective and efficient sanctions screening process". There is an expectation that larger financial institutions should use technology to ensure compliance with regulations and manage the increasing complexity. Technology can help perform the required analysis, as well as the necessary compliance checks. Using appropriate technology solutions and automation can increase efficiency. Recent trends in technology have not only made it easier for institutions to search through vast amounts of data, but have also raised the expectations about the due diligence process, as well as industry standards.

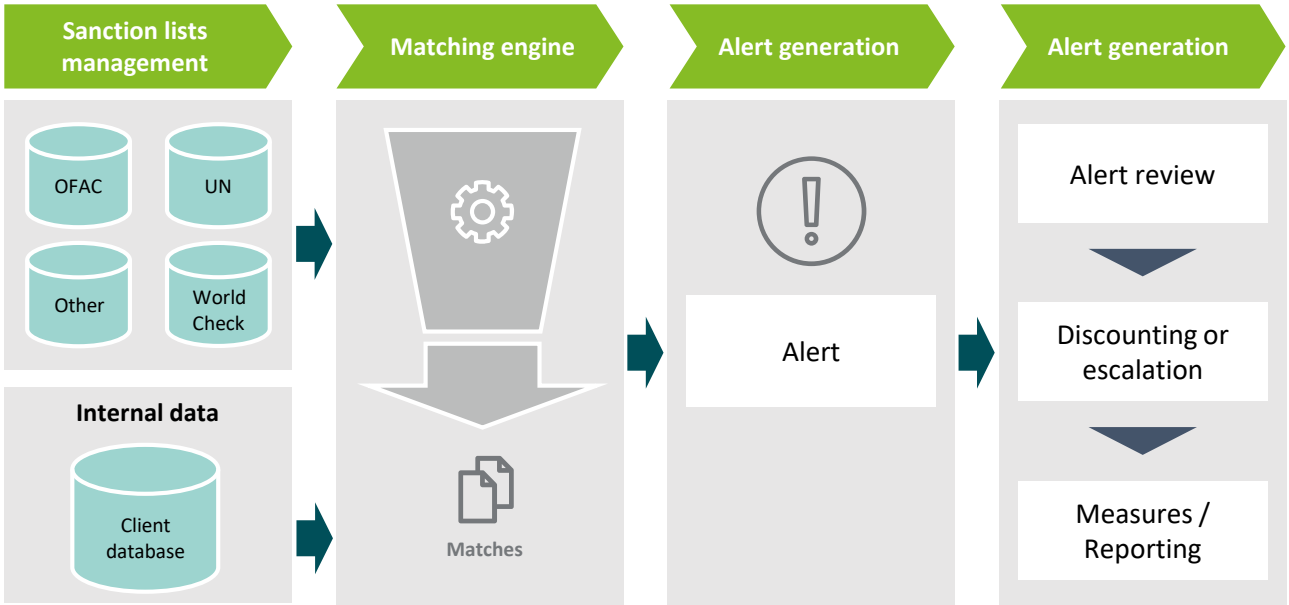
Sanctions are a major part of the global efforts against financial crime. These are directed at states, individuals or legal entities, who are involved (or suspected of being involved) in illegal activities. Governments and institutions such as the UN, OFAC and the EU issue sanctions and restrictions, but financial institutions have the task of implementing them. They are required to search through their client databases and the transactions data to detect any potential violations. Some of the institutions that issue a sanctions list do not have the authority to enforce penalties, such as the UN. However, there are local authorities, such as FINMA in Switzerland who enforce the applicable sanctions regulations.

There is no 'one size fits all' model for a sanctions compliance program that is suitable for all institutions. A model should be designed to allow for factors such as the nature of the institution's business, the countries covered, and the currencies used.

In order for institutions to establish an effective sanctions compliance program, they must first determine the scope of the applicable sanctions regulations. A sanctions compliance program includes two types of screening control: transaction screening and customer screening.

Both types of controls are dependent on a reliable matching engine that compares data from internal and external sources against each other, in order to detect similarities that indicate a possible match. Once a possible match has been identified, an alert is generated. It is then routed to a compliance officer for review, to assess whether the alert indicates a 'true match' or is a 'false positive'. On identifying a true match with sufficient confidence, the institution needs to apply the necessary measures such as blocking a transaction and reporting to the relevant authorities.

The sanctions screening process



An effective data management process has become ever more important for institutions, in order to be able to keep up with the changing sanctions landscape and to remain compliant with their regulatory obligations.

In this thought piece we look at the fundamentals of data management and a potential approach to building a robust sanctions screening program.

2. What is data management?

Data management involves the collection, maintenance, and use of data in a secure, efficient and effective way. Organizations increasingly see data as a key asset for creating value, a robust data management strategy is therefore growing in importance.

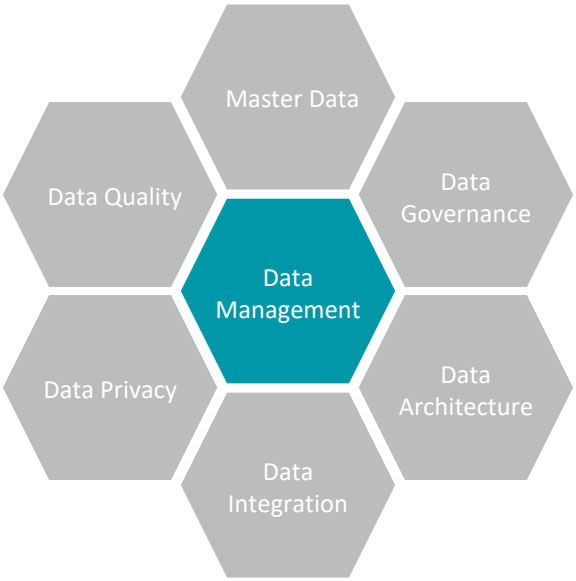
> *"The goal of data management is to help people, organizations, and connected things optimize the use of data within the bounds of policy and regulation so that they can make decisions and take actions that maximize the benefit to the organization".*[4]

A well-maintained data management strategy can help organizations to gain a competitive advantage over their business rivals, as it improves operational effectiveness and decision-making. Organizations that have control over their data can also be more agile, spotting market trends earlier taking proactive measures sooner.

> *"Treating data as an asset can result in diverse benefits, which can be monetized, measured and managed".*[5]

2.1 The sanctions screening process

Data management consists of several elements.



Data Governance

Data governance refers to the set of guidelines (planning, monitoring and enforcement) for managing data assets and making sure that everyone abides by the rules.[6]

Data Architecture

Data architecture is the conceptual structure or framework of the data management environment, its components and interactions. It "interrelates the framework, people, processes, project policies, technologies and procedures to manage and use valuable enterprise information assets".[4]

Data Integration

Data integration is the process of bringing together data from various sources/data collection channels, and putting them into a format for processing.

Data Privacy

Data privacy is concerned with the privacy and sensitivity of the personal data about customers, and procedures for ensuring that personal data is collected, shared and used in appropriate ways.

Data Quality

Data quality refers to the accuracy, completeness, timeliness and consistency of data, together with the requirements and rules for its use. Data quality issues are the cause of most data management. "Without data governance, data quality effort becomes a costly one-off exercise". In order to assure the quality of data, it is necessary to understand its purpose, action, context, and how it is measured.[4]

Master Data (Management)

In a business context, master data is the core data within a system. It is not transactional in nature, although it can include records of transactions. It represents an organization's most valuable data assets. The purpose of master data management is to provide processes for the collection, aggregation, matching and consolidation of data. Master data represents an organizations' "single-source-of-truth" for a specific data set and ensures a common understanding.

3. The importance of a data management cycle for effective sanctions screening

The Wolfsberg Group principles states:

> *"Sanctions screening is used in the detection, prevention and disruption of financial crime and, in particular, sanctions risk. It compares data sourced from a financial institution's operations, including as customer and transactional records from structured (KYC) as well as unstructured (product documentation, client notes) sources, against lists of sanctioned names and other indicators of sanctioned parties or locations".*[7]

Since financial institutions process large volumes of client and transaction data on a daily basis, screening this data against relevant sanction lists can be a challenging task.

Financial institutions are obliged by the regulations to ensure that they will not have a relationship with individuals or entities that are present on the sanction list and neither with entities that are owned by or linked to sanctioned persons and entities. This is not an easy task, as many individuals use similar names, resulting in large amounts of false positives. Peripheral information, such as geographic locations, addresses, occupation, or date of birth may be used to determine the accuracy of a match – data completeness and quality increase the possibility of confirming a true match.

Financial institutions are also obliged to screen high-risk transactions going through customer accounts, in order to ensure that customers do not transfer money to or from sanctioned individuals, entities, jurisdictions or business sectors. Each institution should decide which types of transactions and which attributes within them are relevant for sanctions screening. Beneficiaries and senders of transactions are relevant for list-based sanctions programs, whereas addresses are more relevant for screening against geographical sanctions programs. Other common transactional attributes used for screening include vessels, agents, intermediaries, and free text fields such as payment reference information or the stated purpose of the payment in field 70 of a SWIFT message.

3.1 Sanctions screening data management

Screening controls rely on both internal and external data sources. Some of the key internal data sources across geographical locations and business sectors are master (customer) data, transactional data and other business sector-specific customer information. External data sources include sanctions lists and additional indicators of sanctioned parties. Additional external data sources such as public registers, government lists or other reliable independent licensed sources for data enrichment may also be used for screening.

Data sources are often distributed across multiple IT systems and must be identified in order to be able to assess which elements of data are needed for the screening process. The purpose of data identification is to obtain a holistic view of the institution's customer base.

It is important that all data sources can be linked and integrated at the most granular level possible, and should have the same quality standards.

Before customer, reference or transactional data can be used for screening, it must be extracted, enriched, mapped, transformed and/or loaded into a single platform. If data is corrupted or compromised in the process, sanctions screening model will not operate as intended. The 'Supervisory Guidance on Model Risk Management', issued by the Office of the Comptroller of the Currency (OCC), states: "Process verification includes verifying that internal and external data inputs continue to be accurate, complete, consistent with model purpose and design, and of the highest quality available".[8] Financial institutions should therefore ensure that data quality, completeness and integrity is tested, documented and monitored on a regular basis.

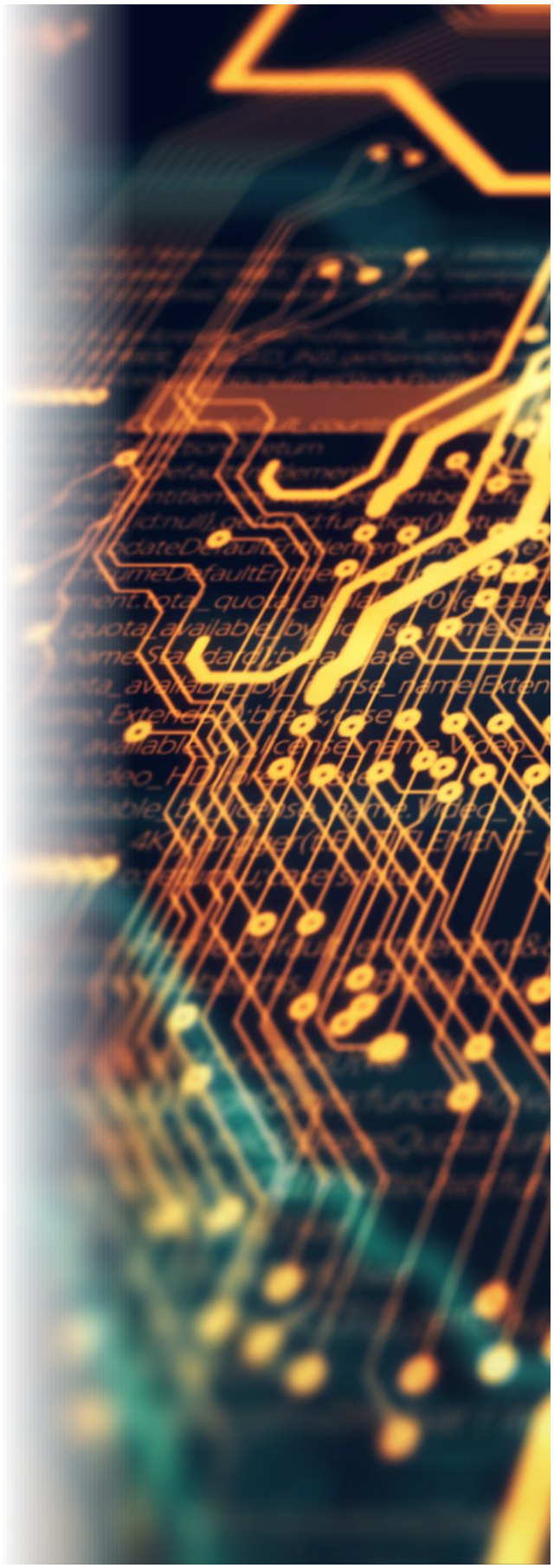
3.2 Sanction lists management

While it may seem that sanction lists are simple and straightforward, in practice they involve large amounts of varied data, including not just the names of listed entities and individuals but also additional details such as known abbreviations, acronyms, aliases, and geographic locations. In order to establish an effective management process, institutions should clearly define who is responsible for the delivery and maintenance of sanction lists.

The first step in the sanctions list management process is to determine and prioritize the lists deemed relevant for screening. These may be externally sourced lists from third party list providers or lists from regulatory websites (e.g. OFAC, UN, EU) as well as internal lists of individuals, entities, regions, ports or prohibited goods. The selection of lists depends on various factors such as type of clients, products offered, and nature of the business. In order to select relevant lists, financial institutions should complete a risk-based assessment and take into consideration relevant regulatory requirements.

Financial institutions that use external vendors for sourcing and maintaining regulatory sanction lists should have a formal process for reconciling its third party-provided lists with regulatory lists, to ensure completeness.

On the other hand, financial institutions relying solely on sanction lists from regulatory websites must ensure that their process should involve consolidating data from multiple sources, which may be in different formats. In addition, some individuals/entities will be included in more than one list, so it is necessary to remove duplicates as not doing so may cause an alert to be generated twice. In such cases, the financial institution should consider implementing a sanction list management system to clean, parse and format the list data in order to improve matching accuracy and reduce number of false positives.



4. Challenges in managing data for sanctions screening

Financial institutions face many challenges to data management for sanctions screening purposes. Here are some examples:

Screening of politically exposed persons (PEPs) and persons related to PEPs

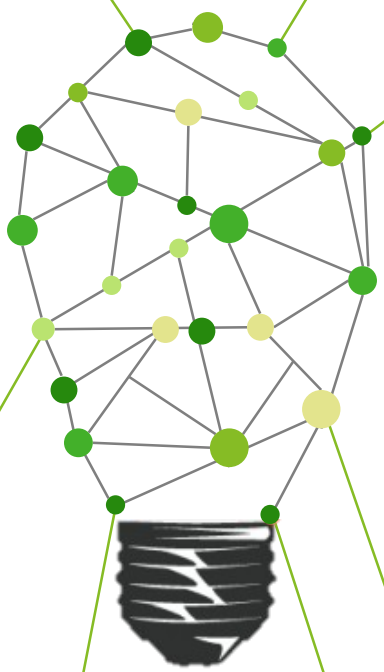
Although government regulations like the Fourth European Union Anti-Money Laundering Directive or FATF recommendations provide detailed requirements relating to PEPs there is no clear way of identifying PEPs and their associates around the world. There are many third party providers of PEP databases; however it can be difficult to use the information they contain to match correctly a financial institution's customer with a PEP. In response to the scrutiny that is be placed on them, PEPs try to find ways to avoid detection, such as opening accounts in the name of corporations (e.g. shell companies) in offshore jurisdictions, instead of in their own names or the names of close family members.

Different writing systems and regional naming conventions

Financial institutions often have to screen customers whose names are on lists that are not originally written in roman characters, but in Chinese, Cyrillic or Arabian, such as suspected terrorists from Middle East countries. Many names of terrorists on the OFAC SDN list also include aliases. It may be helpful to know certain rules about names. For example, many Arabic names begin with the word Abu that means 'father of'. Abu, followed by a noun, means 'freedom' or 'struggle', and is used by both terrorists and legitimate political leaders.

Isolated systems

In many cases, financial institutions' systems are not integrated between its branches and subsidiaries after an acquisition or merger.



Unifying sanctions list

Financial institutions should establish an effective process to ensure that the sanction lists they use in the screening process provide an accurate and complete unified list for screening.

Poor data management

Lack of data completeness, quality and integrity is the main reason for poor performance of sanctions screening systems. Missing or incorrect Know Your Customer (KYC) information, or missing information on company shareholders, beneficial owners, suppliers or other counterparties have a negative impact on the effectiveness of screening tools, producing large numbers of false positive alerts or making it impossible to detect sanctioned entities or individuals.

Manual data processing

Customer data is often entered into a banking system manually during the on-boarding process, which in turn increases the probability of errors.

Volume of data

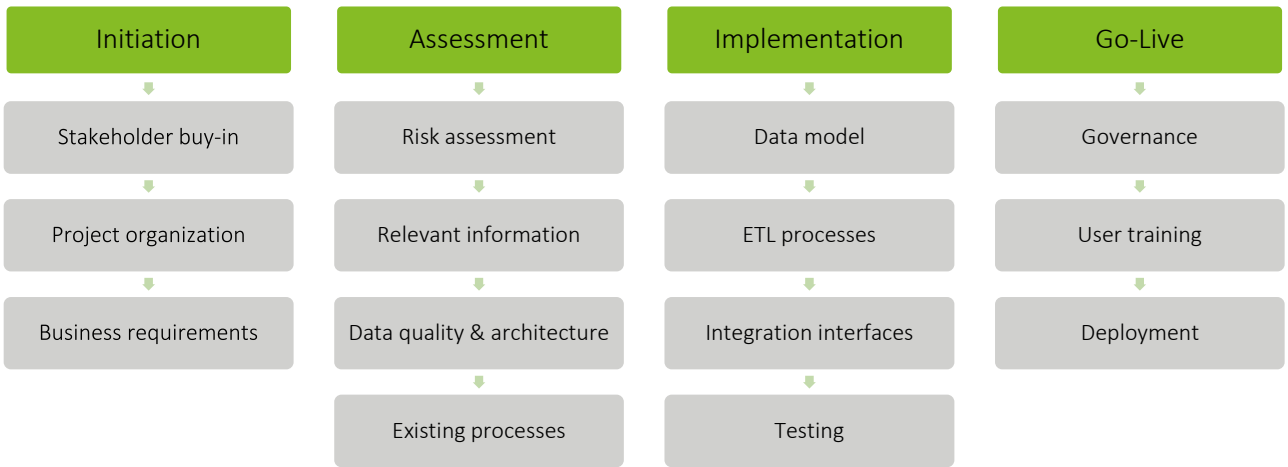
The sheer volume of data involved in a comprehensive sanctions screening process makes a manual processing system very difficult, if not impossible, to operate.

5. Potential solution and its benefits

5.1. Design and implementation

The figure below illustrates the implementation and operation of a solution for financial institutions in establishing an effective sanctions screening process. The solution would need to be partially automated, tailored to specific business needs, and designed with a holistic risk-based approach. The implementation of the solution generally follows a defined process, which consists of the following steps:

The sanctions screening process



Initiation

A top-down approach is required, in which the relevant stakeholders are involved from the very beginning. Technology and a data-driven approach are required to run an effective sanctions screening process. The organization of the project should be defined beforehand in order to be able to involve the relevant stakeholders throughout all phases of the project.

Design and implementation

The data model builds the technical foundation for the potential solution. It should be flexible and expandable. Tailored 'extract, transform, load' (ETL) processes must ensure that up-to-date data is collected and is transformed appropriately. Integration interfaces allow information to be leveraged by relevant business processes.

Assessment

The assessment is based on the business requirements, and addresses associated risks, the quality of the required data and the data architecture, as well as the existing processes that are impacted by the screening system.

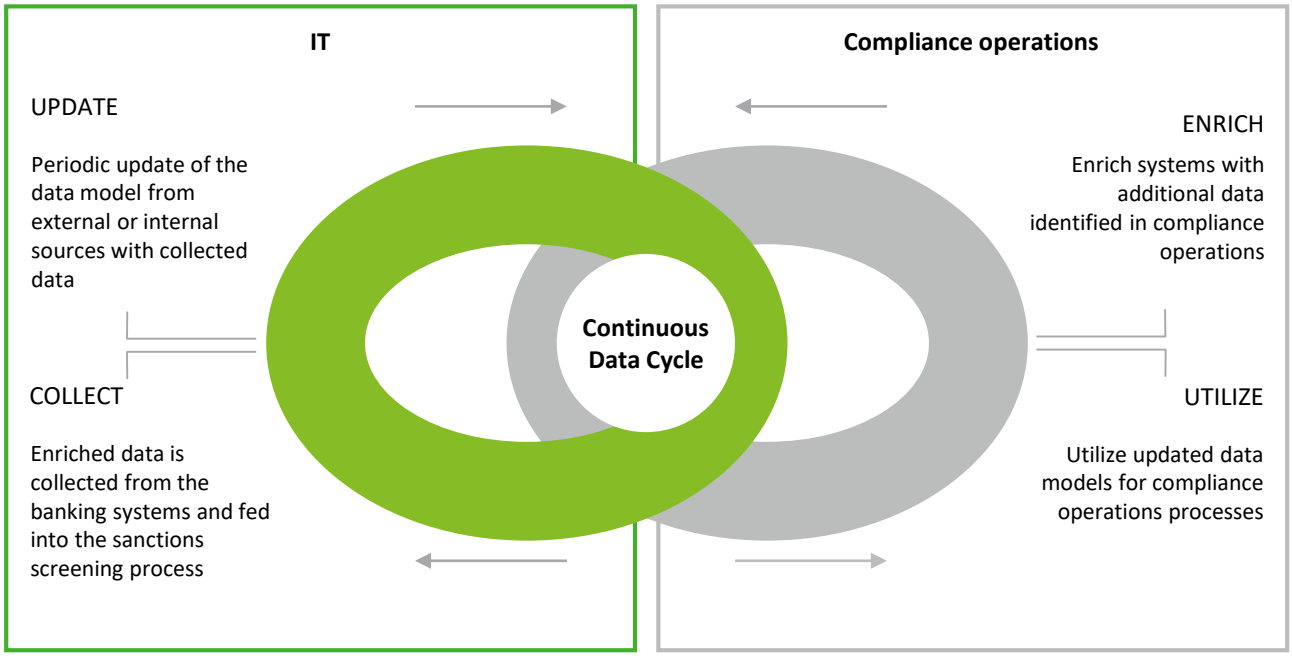
Go Live

Before a technology solution goes live, the process governance must be defined and users must be trained. Another crucial aspect is the deployment and maintenance of the solution, e.g. versioning of the solution in the deployment process to ensure streamlined maintenance and ensure that new versions are deployed correctly.

5.1. Design and implementation

Once it is operating, the system should ensure a continuous cycle of data between the organization's IT systems and the screening system of the compliance department. Data triggered by the sanctions screening process, such as the findings from a related internal investigation or updates to client risk scoring models, should be updated automatically in the respective IT systems. This enables the IT systems to extract accurate data for inclusion in the screening model.

Continuous data cycle for sanctions screening



This diagram shows a framework for a continuous cycle of data management for sanctions screening purposes. Internal data from the organisation's IT systems flow into the screening process, where it is enriched with additional information and then fed back into the IT systems.

To ensure continuity of the process, a data management officer should be appointed to perform an oversight function.

In summary, effective data management and analytics play an important role in detecting and reducing the risk of financial crime. Regulators from all over the world emphasise the importance of implementing new technologies to enhance the sanctions screening programs of financial institutions.

6. Sanctions screening trends

With growing data volumes and an ever-changing sanctions screening landscape, the need for automated processing and cataloguing of data as well as real-time sanctions screening will be 'a must'. Recent trends within large institutions point to the deployment of a more holistic approach and greater use of available data.

> *"Information sharing is critical for combatting money laundering, terrorist financing and financing of proliferation. Barriers to information sharing may negatively impact the effectiveness of AML/CFT efforts. This underscores the importance of having rapid, meaningful and comprehensive sharing of information."*[9]

7. References

[1]"AML, KYC & Sanctions Fines for Global Financial Institutions Top $36 Billion Since Financial Crisis", Fenergo, 2020, https://www.fenergo.com/news/aml-kyc-and-sanctions-fines-for-global-financial-institutions-top-$36-billion-since-financial-crisis.html

[2]"Banks adopt AI to manage sanctions and compliance risk", A. Ross, 2020, https://www.ft.com/content/98e82234-16a8-11ea-b869-0971bffac109

[3]"Standard Chartered fined $24.9M for Ukraine sanctions breaches", N. Hodge, 2020, https://www.complianceweek.com/sanctions/standard-chartered-fined-249m-for-ukraine-sanctions-breaches/28686.article

[4]"What Is Data Management?", Oracle, 2020, https://www.oracle.com/database/what-is-data-management/

[5]"Data integration: after the teenage years. Recruit Institute of Technology", B. Golshan, A. Halevy, G. Mihalia, W-G. Tan, 2017, https://dl.acm.org/doi/pdf/10.1145/3034786.3056124

[6]"Big data privacy: a technological perspective and review. Journal of Big Data ", P. Jain, M. Gyanchandani, N. Khare, 2016, https://journalofbigdata.springeropen.com/track/pdf/10.1186/s40537-016-0059-y

[7]"Wolfsberg principles on sanctions screening", The Wolfsberg Group, 2019, https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf

[8]"Supervisory Guidance on Model Risk Management", Office of the Comptroller of the Currency, April 4, 2011, https://www.occ.gov/news-issuances/bulletins/2011/bulletin-2011-12a.pdf

[9]"FATF Private Sector Information Sharing Guidance", Financial Action Task Force, November 2017, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf

8. Contacts

Bob Dillen
bobdillen@deloitte.ch
P: +41 58 279 69 29
M: +41 79 908 70 06

Uday Mehta
udmehta@deloitte.ch
P: +41 58 279 66 84
M: +41 79 417 08 49

Michel Nyffenegger
mnyffenegger@deloitte.ch
P: +41 58 279 84 27
M: +41 79 544 33 29

Katarzyna Michalowska
kmichalowska@deloitte.ch
P: +41 58 279 62 63
M: +41 79 896 31 35

Michelle Rosenberger
mrosenbergerlomeli@deloitte.ch
P: +41 58 279 60 06
M: +41 79 857 68 23

Designed by CoRe Creative Services. RITM0500675