AML and Data Governance: How Well Do You KYD?

POWERFUL INSIGHTS

Issue

Financial institutions have invested significant time, money and resources into developing and maintaining anti-money laundering (AML) compliance programs. One key enabler of an AML compliance program is the software used to review customers, analyze transactions to identify suspicious activities, and provide analytical and research capabilities to support the filing, or non-filing, of suspicious activity reports (SARs). Another important component of an AML compliance program is "know your customer," or KYC, activities. These are the activities performed by financial institutions to establish the identities, gain knowledge about the expected transaction activity, and risk-rate its customers. Both of these critical processes rely on the quality and accessibility of data. Yet, financial institutions often overlook another key tenet of effective AML compliance – "know your data," or KYD.

KYD is not just about providing definitions and broad-stroke understanding of data. It requires knowledge of data lineage, systems, storage, and the way the data is leveraged across different AML processes. For AML professionals already stretched and weary of continuing scrutiny, becoming proficient in data management may sound like a lot of extra work – adding yet another layer of complexity to an already difficult job. Still, AML departments stand to benefit the most from KYD activities and improved data management.

Data governance is the best approach to combining these three components – the sophisticated software applications, the knowledge of what the customer needs, and the accurate understanding of data definitions for inputting the appropriate data. Data governance efforts are viewed well by regulators, who increasingly put pressure on financial institutions to formally document business processes, data controls, source-to-target mapping, and defend all activities around data management.

For many organizations, meeting these expectations may seem daunting. It is, therefore, important for institutions to define their objectives clearly when designing a data governance function for AML or any other purpose, and

scope the undertaking appropriately to help them achieve their specific goals of managing, protecting, ensuring quality, and, ultimately, knowing their data.

Data governance is a wide set of management and technical disciplines designed to ensure that an institution has the right data available at the right time and that the data is accurate and in the correct format required to satisfy specific business needs. Much like AML compliance generally, technology enables the process, but it is specific business knowledge and context being applied to a set of information that really adds the value.

While technology platforms are certainly enablers in supporting this governance (e.g., data quality monitoring, centralized data dictionaries), AML leads must work closely with first-line process owners to ensure a good definition, ownership and monitoring of key data assets required for the AML programming. Technology components supporting this include the management of master and reference data, which helps to ensure uniformity and improve quality across data sets flowing from diverse systems. From a transaction monitoring process standpoint, a single customer with multiple accounts and conducting multiple types of transactions will have the customer name, transaction details and other identifying information appear in multiple records, across multiple systems. The process of consolidating this information into a single customer record for transaction purposes (to prevent the same customer from generating duplicate alerts) can be facilitated through strong reference and master data management. The technology, a key component of AML compliance, cannot work effectively without this kind of maintenance of the information that is fed into it. This is where data governance is key.

Challenges and Opportunities

For an organization's data to meet the AML challenge in just the area of transaction monitoring, available data must include the in-scope transactions and all the attributes needed for monitoring. This information must be captured

and analyzed in a timely manner, and it must be clearly understood by the AML team to attest to the validity of monitoring rules and to support decisions around potential SARs and other regulatory filings. This challenge is not insurmountable, but it can be significant, due to the way many financial institutions grow their business (e.g., through mergers and acquisitions), often resulting in siloed organizational and technical infrastructures with redundant and difficult-to-integrate systems and data stores. Making sense of the data resulting from these mismatched systems is a tall order for many institutions, which not only need to ensure the data flowing into AML systems or databases is complete and accurate, but also need to be able to interpret this data within the context of their business needs.

Putting data into the context of an institution's business needs requires understanding of the business definitions of specific data elements, the way those elements are used within specific business processes across the enterprise, the individual systems or databases that house the elements, and any business rules or transformations that occur on the data. This requires complete knowledge of both business and technical metadata to provide a full view of the lineage and proper use of key data elements. To possess such cradle-to-grave knowledge of data, institutions need to be able to answer the following questions:

- What system did the data come from and what up-front controls exist within those systems to protect the quality and fidelity of the data?
- Can the data be linked back to the first-line business processes to ensure that the right data elements are being leveraged for transaction monitoring?
- Is there data quality monitoring in place to flag issues such as incomplete transactional data or material changes in volume?
- Does similar data from different data sources actually mean the same thing throughout the business?

An effective data governance program should provide the answers to each of these questions, and many more. To establish such a program and framework, financial institutions first need to overcome several typical challenges, listed in the table below:

Typical KYD Challenges
Lack of understanding of data – As financial institutions continue to grow and acquire and/or update data sources, the enterprise and AML data governance team may fail to take into account the downstream impacts to various applications, resulting in ineffective data usage. Understanding the data requires not only knowledge of the technical lineage of the data, but also the business knowledge to understand how the data is used within key business processes and across the organization. This is one of the main reasons the AML compliance department needs to drive, or at least be a key player, in the effort to understand data.
Data quality gaps – Many front-end systems and business processes capturing data for AML may not populate key data elements (e.g., country of domicile, ISIN, counterparty) uniformly, or may capture this data in free-form fields or hard-to-leverage formats. This limits the ability to use this data for high-volume transaction analysis, leading to potential false positives or overall misses in the identification process.
Lack of a centralized data dictionary and metadata – Many financial institutions do not have dedicated resources (people and processes) who can act as data stewards and can educate the downstream users on data changes as well as decide how best to harness the data. Such data stewardship is a key requirement in getting to KYD.
Technological gaps and challenges – Financial institutions are already inundated with both structured and unstructured data, and the data flow is ever-increasing. Without common data repositories/warehouses to support seamless integration, technology organizations are unable to meet the business demands to integrate, process and sort this data on a timely basis. Frequently, businesses attempt a solution through building data processes outside of IT ("shadow IT" solutions). Unfortunately, this approach often exacerbates the problem. Many times, these unsanctioned sources lack uniform master or reference data, may be using outdated, inaccurate information, or may not have data of sufficient granularity.
Management silos – Larger institutions especially are often plagued by communication gaps among departments. This can make effective data collaboration difficult, and often leads to data duplication, disparate data processes and multiple versions of data transformation logic. All of these issues make it difficult to centralize functions for AML compliance and result in ineffective AML data analyses. KYD is key in integrating these silos by providing the answers to important questions about the data – where it is stored, how it was created, what is its definition, what business rules and standards have been applied to it, and how it is used across the organization.

Our Point of View

KYD is critical to the long-term success of any AML program. In addition, many of the basic tenets of KYD are the foundational building blocks of any data governance effort and are essential to building effective end-to-end business processes. These basic tenets include:

- Defining common data across different products/lines of business, functions and business processes to easily integrate data sets across the enterprise

- Strong governance and management of master and reference data
- Well-defined business processes, controls and documentation
- Complete and accurate business/technical metadata to ensure clear lineage/traceability of data origin
- Key resources (data stewards and owners) who have accountability and responsibility for the management of data quality throughout the data life cycle

Steps to an Effective Data Governance Function

Institute and enforce effective master- and reference-data management programs. This will enable the institution to uncover data structure issues and, in the event of data unavailability, elicit new efforts to source data that downstream applications like AML transaction monitoring systems can leverage to perform a more refined data analysis.

Institute enforceable enterprisewide data governance strategy and processes. The institution will use this strategy to tear down the data silos and create a free flow of data within the enterprise.

Be proactive in assigning data ownership and monitoring of data quality. Assigning ownership and responsibility for key data within the AML processes will help ensure continued compliance. It is important, for example, to determine who has the responsibility to inform the AML monitoring team when new products or customer types are added into source systems. It is also important to provide tools for continuous monitoring of data quality and to assign responsibility for any problems that may arise with the data.

Create a centralized repository for metadata. A centralized repository will help the institution gain an understanding of redundant data processes and eliminate them. This will streamline downstream consumption and lead to reduction in the total cost of ownership of various data sourcing applications. IT will also allow new data processes to be less time-consuming and cheaper to implement due to clearer understanding of the data that is available to support the processes.

Support big data initiatives. Financial institutions are deluged with new data daily, and the ability to incorporate new ways of monitoring the large volume of transactions and extract value from the data is critical to effectively managing and maturing AML programs. It is important for institutions to maintain strong data governance as it allows institutions to transition easily to big data analytical platforms and tools through easier data integration.

Luckily for AML teams, some organizations have begun to take the steps above and implement data governance to satisfy other regulatory or compliance requirements (e.g., Comprehensive Capital Analysis & Review [CCAR], Solvency II, and Basel Committee on Banking Supervision Principles for Effective Risk Aggregation [BCBS 239]). These efforts can easily be leveraged by the AML teams. With or without these other programs, AML teams should ask the following questions:

- What processes do we want data to support?
- What data is available to us?
- What data is still needed?

- What is an acceptable level of data quality, and who is ultimately responsible for ensuring the data is delivered at that quality?
- How will we keep this data updated, and respond to changing systems and technology across the organization?
- Where does AML compliance fit in the technology hierarchy?

By answering these questions, financial institutions will begin creating a solid foundation for data-driven AML compliance.

PROVEN DELIVERY

How We Help Companies Succeed

Protiviti's team of dedicated professionals provides clients with solutions in AML compliance and data governance. We help organizations design data governance programs from the ground up to support not only the appropriate and effective software, but also the components needed for KYC and transaction monitoring efforts. Protiviti's subject-matter experts have teamed with AML compliance functions to execute a variety of unique, enterprisewide master and reference data management projects.

In addition, we offer solutions that leverage the unique skill set from our AML and Data Governance practices:

- Enterprise data governance design and implementation
- Customer risk-scoring methodology design and implementation
- AML systems architecture and data governance assessments
- AML systems validation and tuning
- Master data and reference data management design and implementation
- Data quality index (DQI) design and implementation
- AML alert production testing and SAR regression analysis
- Industry benchmarking

Example

Recently, Protiviti successfully partnered with an organization to determine how it could support a centralized customer information repository that would serve as a uniform data source for all customer-related information, including risk rating. We began by identifying governance deficiencies and then worked with the client to build a corrective action strategy that addressed not only the storage of customer information, but also resolved breakdowns and limitations in both the customer risk scoring and subsequent transaction monitoring processes.

Through the collaboration between the client's AML function and the Protiviti team, it was revealed that there were substantial data integrity and completeness issues across the core systems supporting transaction monitoring. The issues could have been avoided if effective data governance practices were in place. Because these practices were not implemented earlier, the bank was criticized significantly during an AML compliance program examination.

The Protiviti team brought together the AML compliance function personnel and data stewards from the business side to launch a strategic initiative to expedite remediation. Through the implementation of the key data governance principles, Protiviti helped the client formulate an effective and proactive resolution and avoid an enforcement action.

Contacts

Carol Beaumier
+1.212.603.8337
carol.beaumier@protiviti.com

Matt McGivern
+1.404.926.4346
matt.mcgivern@protiviti.com

Shaheen Dil
+1.212.603.8378
shaheen.dil@protiviti.com

Chetan Shah
+1.704.972.9607
chetan.shah@protiviti.com

About Protiviti

Protiviti (**www.protiviti.com**) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Named one of the 2015 *Fortune* 100 Best Companies to Work For®, Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®
Risk & Business Consulting.
Internal Audit.