





# Anti-money Laundering and Data Quality

by Julie Steinberg

**FINANCIAL INDUSTRY EFFORTS TO PREVENT** money laundering and detect financial crime have changed dramatically in the aftermath of the Sept. 11 terrorist attacks. Prior to Sept. 11, government and industry Anti-money Laundering (“AML”) regulation targeted monetary proceeds of drug-related activities and illicit businesses.

AML regulation focused primarily on banks. Many financial institutions complied with basic AML and minimum KnowYourCustomer (“KYC”) standards. Comprehensive financial crime prevention among most banks was an exception rather than a rule.

Post Sept. 11, AML regulations (enacted by the USA PATRIOT Act of 2001) are broad, comprehensive and probing. Almost all financial institutions and intermediaries (not just banks) must implement AML programs that can detect unusual transactions, identify customers and prevent financial crime. Financial service organizations face strict guidelines and many are unprepared for meeting the demands of enhanced compliance with complex regulations. Specifically, organizations must augment KYC capabilities to meet enhanced reporting and recordkeeping regulatory requirements. The creation, management and use of customer and transaction data are a crucial challenge for most institutions.

*Organizations must consider the quality of the data that they provide to internal and external teams, including Compliance, Treasury, Internal Audit, External Audit, and Regulators. Such data must reflect accurately an organization’s customers and related transactions.*

## **Getting to Know You**

Although regulatory issues are often delegated to an organization’s Compliance unit, many regulatory risks impact an entire enterprise. Therefore, Compliance Departments as **consumers** of data need to be confident that the Operations and Front Office teams, or **producers**, have entered data that meets agreed upon levels of quality. Similarly, Compliance units need to be confident that Information Technology (IT) will act as effective data **custodians** by maintaining data that is organized and accessible. Importantly, if regulators request data, it must be accurate.

Reliable KYC information is supported by accurate measures that classify and risk rate customers, based on complex matrices driven by key customer data. Matrices vary by organization and are developed based on individual requirements and characteristics. Customer data types used to complete a KYC risk matrix may include control country, customer type, customer transaction types and customer size. In order to meet basic Bank Secrecy Act requirements, organizations must maintain customers' legal address and tax ID to validate transactions.

***Almost all financial institutions and intermediaries (not just banks) must implement AML programs that can detect unusual transactions, identify customers and prevent financial crime.***

KYC data is prone to human and system errors, poor control environments and security flaws. Until Sept. 11, KYC data had not been a priority for many financial institutions. Instead, it was a by-product of business processes such as account opening, transaction processing and tax reporting. Because such processes rarely share common goals, priorities or owners, KYC data requirements and quality could be inconsistent and of poor quality.

So, how does a Compliance unit determine that KYC reports, comprised of customer data and provided to Internal/External Audit, the Board and regulators, are accurate? What constitutes accurate KYC data? Which standards should be applied to past, present and future KYC data? What does an organization really need to know about its customers?

**Data Quality and KYC**

Data quality refers to a process for ensuring that information is correct, complete, accurately reported and effectively organized. PricewaterhouseCoopers' Data Quality Methodology can help clients assess, identify, measure and resolve data quality issues. When searching for a data quality/KYC solution, consider the following:

■ Data needs to be reviewed at the field level. Assess the 15 or 20 most important KYC fields by performing a data profiling and analysis exercise, and identify major issues. Findings from a data profiling exercise might include:

- Customer tax ID's are not found within the system.

- Customer address information is not always entered in the same field and format. Alternatively, a customer's address is incorrectly entered as "123 4th Street" instead of "12 34th Street."
- It is difficult to identify American customers because the system permits free text data entry responses, including "USA," "United States," "US," "America," etc.
- There are inadequate transaction classifications.
  - Transactions are entered in local currencies, but stored as U.S. dollars.

■ Once the data has been profiled, organizations must benchmark data quality by consensus. A Compliance unit will have very different ideas of requisite KYC data quality than the Front Office, Operations or IT. An organization should set agreement on levels of data quality for KYC elements.

■ Organizational ownership for data quality should be assessed. Producers, consumers, and custodians need to take responsibility for KYC data. Data stewards should be appointed to assume day-to-day responsibility for KYC data quality.



- KYC data cleansing should be approached cautiously. Organizations should consider the impact this effort will have on other business areas and processes, and proceed by order of priority and number of dependencies.
- Controls can be implemented, but only if the data problems have been properly identified and assessed. Using the Data Quality Methodology, organizations can develop data quality sustaining measures to ensure that requisite data quality can be monitored, appropriate policies and procedures developed, and key systems controls implemented.
- AML/KYC software solutions are effective only to the degree that underlying source data is accurate and consistent. Before purchasing AML analytical software, organizations should

ensure confidence in KYC data such software will analyze. A conservative rule of thumb is that data costs will be at least twice those of the software itself.

Lastly, data quality is an enterprise risk issue. By use of Data Quality Methodology, organizations can promote KYC data integrity strategies to mitigate regulatory risk, prevent money laundering, deter financial crime and avoid inadvertent assistance to criminals, terrorists and their allies.

---

**For more information on anti-money laundering and data quality, please call Julie Steinberg in New York at (646) 471-3501 or [julie.steinberg@us.pwcglobal.com](mailto:julie.steinberg@us.pwcglobal.com).**

---

