ACAMS® TODAY

The Magazine for Career-Minded Professionals in the Anti-Money Laundering Field

Financial Institutions have often realized the importance and benefits of good data quality. The fact is that most of these organizations struggle with data quality issues. The costs associated with poor data quality are not only ignored but budgeted into the overall category of the cost of doing business. However, a financial institution can eliminate these costs and insure proper regulatory compliance by instituting a data quality improvement program as a core component of its overall business intelligence strategy.

According to an August 2009 survey conducted by the research firm Gartner "The average organization loses about $8.2 million annually through poor data quality." Further, of the 140 companies surveyed, 22 percent estimated that bad data caused annual losses of $20 million. Four percent estimated as much as $100 million. The compliance costs could be much higher in terms of reputational risks, enforcement actions and penalties, as well as higher allocation of resources to remediate the data quality.

Regulators have specified that good data quality is part of the overall risk and compliance process. The European Union's Third Directive on anti-money laundering (AML) and the USA PATRIOT Act have both focused on data quality in the following areas:

- Customer Identification Program (CIP)
- Know Your Customer (KYC)
- Customer Due Diligence

Of particular interest is Section 319 of the USA PATRIOT Act that requires a foreign financial institution that maintains correspondent accounts in the U.S. to provide full details for any account it holds within five calendar days upon receiving a request from a federal agency. This means that the financial institution must be able to locate and provide comprehensive data on any of its accounts in a timely manner. This is possible only if the organization has developed a system for assuring data quality.

Perhaps most significant is the risk that true suspicious, fraudulent, or other illegal activity is occurring within a financial institution and is not detected. The over used saying "garbage in — garbage out" is as true for a compliance solution as it is for any other automated system. Rules, profiling, peering and other detection strategies will yield incorrect results if they operate on incorrect or missing data.

Causes of poor data quality

There are many factors that lead to poor data quality. To uncover causes and assure that an organization is achieving an adequate level of quality, an appropriate review is required. Nevertheless, some causes of poor data quality commonly are:

- Legacy data from other systems (core banking system or KYC system) has not been reviewed or updated in a very long time
- Most legacy systems have only rudimentary data quality business validation rules which often results in errors and inconsistencies from staff responsible for data entry and data validation
- Inefficient processes in managing or maintaining data
- Mergers and acquisitions often lead to

IDOLA INFOTECH

consolidation of systems, which cause data compatibility issues such as duplicate customers, lack of data standardization, etc.
- Lack of proper training for the staff responsible for gathering and entering data
- Data mapping between the core banking and transaction monitoring systems, undertaken by IT staff without compliance involvement or IT staff not having a full understanding on compliance requirements would often result in data mapping issues

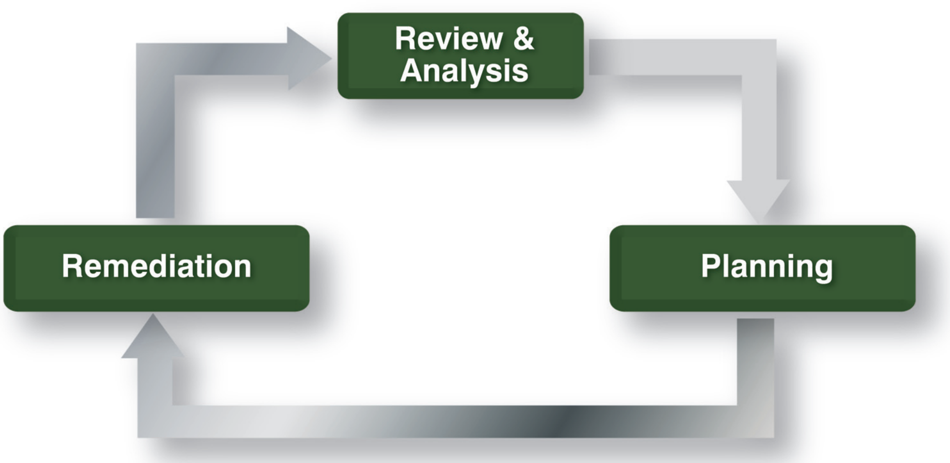
The impact of poor data quality

Poor data quality affects compliance in the following ways:

- Most financial institutions adopt a risk-based approach to identify the risk posed by the institution's customers. If the information is not accurate or complete, the risk classification of the customer will also be inaccurate
- Poor data quality results in inefficiencies in suspicious activity monitoring and detection. This translates to high false positives or missing out on genuine suspicious activities
- Poor data quality results in more time taken for case investigation resulting in inefficiencies in cases review process
- The data contained in the Suspicious Activity Reports (SAR) will often be inaccurate or incomplete. Law enforcement agencies often stress the importance of quality data on SARs filed
- A financial institution will not be able to demonstrate a sound monitoring program to the regulators which could result in enforcement actions, expensive look backs and reputational risks

A framework for data quality

The following diagram depicts Idola's framework for improving data quality which involves the following processes:



Review and analysis:

- Review business artifacts to understand the compliance requirements
- Review mapping documents and interface specification documents between data sources and transaction monitoring system
- Identify the data sources that feed data into transaction monitoring system
- Identify gaps in data accuracy and incidences of non-conformance
- Perform "data profiling" to understand the data and identify areas of improvement

Planning:

- Define targets and prioritize them. Set targets to improve data characteristics like completeness, consistency, accuracy etc.
- Obtain buy-in from stakeholders and business process owners that manage data
- Define metrics to benchmark data quality based on "data profiling"
- Allocate resources

Remediation:

- Automate manual processes where possible to drive data quality and gain efficiency
- Implement tighter integration of systems such as core banking system, KYC and the transaction monitoring system
- Implement process improvements by identifying deficiencies in existing process for data collection
- Implement training programs that focus on personnel involved with data collection
- Use data cleansing and data enrichment tools to enrich data that needs improvement
- Use trusted third-party reference sources for data validation and enrichment

Benefits from improved data quality:

Perhaps the most important benefit from assuring appropriate compliance data quality is its significance in mitigating the threat of reputational risk. It is regrettably all too common to read in the newspapers examples of banks under severe regulatory pressure from enforcement actions. Inevitably, this leads to deterioration in confidence from clients and shareholders.

Other key benefits from improved compliance data quality include:

- Ability to demonstrate a sound monitoring program
- Improvement in operation efficiency and reduced cost
- Improvement in customer satisfaction and retention levels
- Ability to keep up with changing regulations
- Ability to expand business in new areas thereby resulting in revenue growth

Financial Institutions should understand that poor data quality is not just an IT problem but a business problem. The business process owners that manage data should be empowered to ensure that data quality is maintained. Financial institutions must create a "data culture" and establish a mindset that data quality is everyone's responsibility, an ongoing effort and should be treated as an institution's asset to achieve better results.

Conclusion

With the convergence of enterprise risk, fraud and AML compliance, the need for financial institutions to access clean, accurate, standardized and timely data has gained importance. Banks and other financial firms need to invest in improving data quality, which should not be viewed as a cost to the institution. High-quality data can be achieved through a combination of people, process and technology. The availability of good quality data will enable financial institutions to meet the ever-changing regulations, be it on the enterprise risk or on the AML compliance side.

Maintaining good data quality is beneficial to any organization but is especially relevant for compliance in demonstrating a sound monitoring program. Maintaining good data quality is not a onetime activity — it is an ongoing process.

Rama Pappu, managing partner, Idola Infotech, LLC, Iselin, NJ, USA, ramapappu@idolainfotech.com