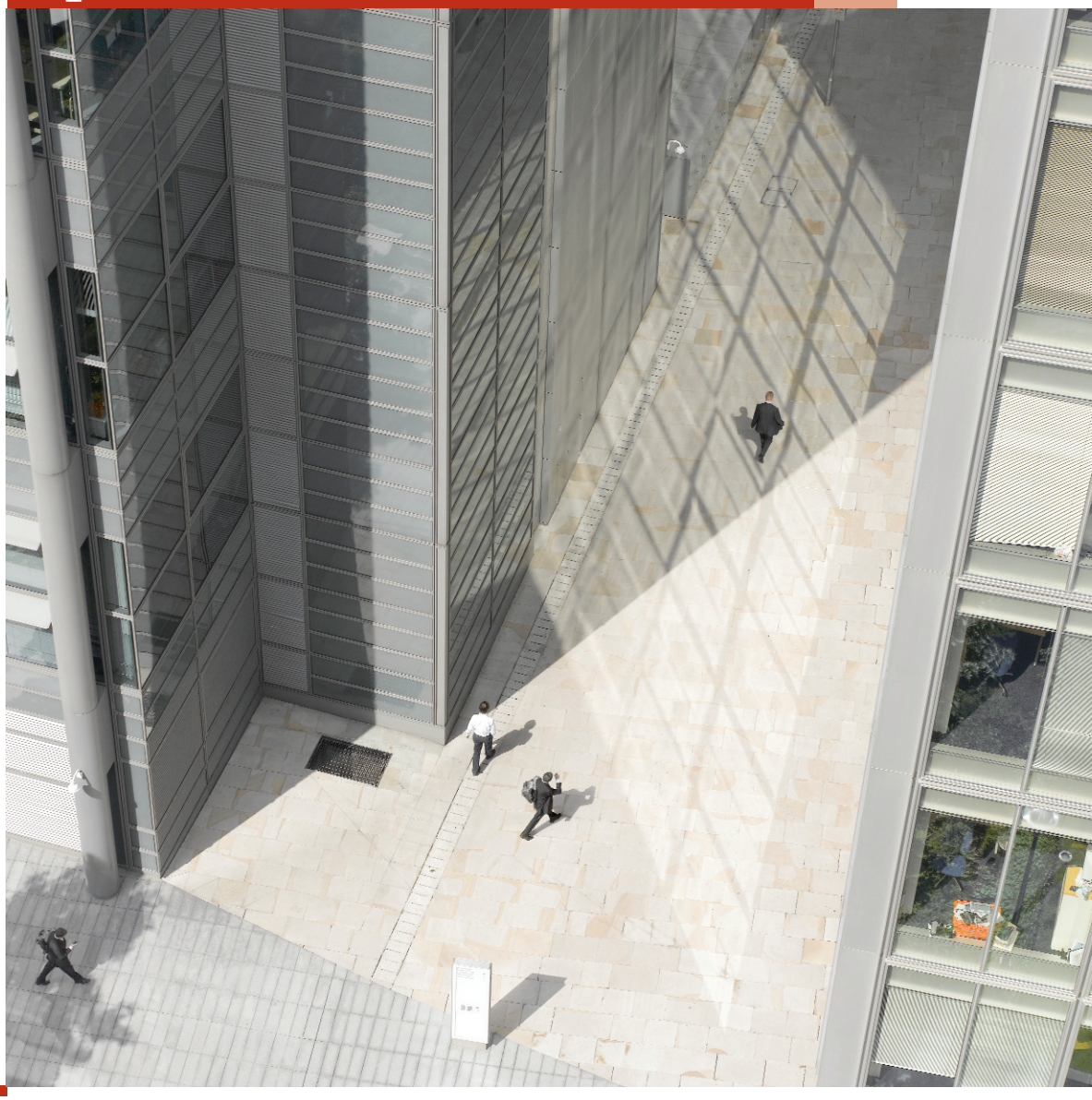
www.pwc.com/us/banking

From source to surveillance: the hidden risk in AML monitoring system optimization

September 2010



pwc

Contents

The heart of the matter

Actively managing AML monitoring data can reduce costs, save time, avoid regulatory remediation, and improve assurance

As the financial crisis levels off, regulators are now refocusing their efforts on anti-money laundering (AML) and terrorist financing enforcement. This increase in regulatory scrutiny is compelling many financial institutions to take a closer look at their AML operations as they seek innovative ways to meet regulator expectations and reduce costs in an uncooperative economic environment. Considering the regulatory complexity and high costs associated with AML transaction monitoring, institutions often start with improving the effectiveness and efficiency of their automated AML transaction monitoring alert engines. When properly configured, these systems can help institutions detect patterns of activity that may indicate money-laundering or terrorist-financing activities.

Poorly defined alert engine parameters and thresholds, however, may raise flags unnecessarily or even miss significant money laundering activity. PricewaterhouseCoopers (PwC) analysis indicates that 90 percent to 95 percent of all alerts generated by AML alert engines are false positives. These high false-positive rates lead to significant monitoring costs but more disconcerting are the false negatives, or the cases of money laundering that are not detected. Unlike false positives, these are hidden, are harder to quantify, and can have significant negative impact. Both of these issues can be addressed if institutions refine their rule set thresholds. But tuning without first tackling AML data quality can lead to skewed and misrepresented thresholds. By the time the data is discovered to be inaccurate or incomplete, a threshold change may have already been implemented, leading to costly rework and the potential for a regulator-mandated transaction lookback. Many institutions are caught in a cycle of tuning, rework, lookback, tuning, rework, lookback, etc., because data quality issues are addressed haphazardly instead of systematically.

The quality of data clearly affects the quality of the alerts generated by a transaction monitoring system. Active management of monitoring data is paramount to improving data quality. When AML transaction monitoring systems were initially implemented, the accuracy of the transaction code data and rules that determined what qualified as an exception may have been established and vetted. Since the original implementation, however, many institutions have not reassessed and verified whether the transaction codes and data that feed their AML monitoring systems remain at initial quality levels. Despite this, many institutions have still spent time and money tuning monitoring rules using outdated, inaccurate, and incomplete transaction reference data. This reliance on a one-time assessment of data ignores an institution's dynamic fiscal landscape as it introduces new products, consolidates financial entities, and its IT infrastructure evolves.

To establish complete and accurate AML monitoring data, institutions should consider a solution that combines transaction code reference data management with a transaction reconciliation utility. Data management is the formal transaction code AML classification process that includes compliance conclusions reached for each transaction code (i.e., whether or not the transaction code should be excluded or included in AML monitoring and why) and the preservation of the nature and extent of the compliance review procedures performed. The transaction reconciliation utility provides recent transaction reconciliation and exception reports between source and surveillance systems to evidence effective system transaction flow. By addressing the quality and consistency of transaction code data, institutions can save time and money, avoid substantial fines and costly remediation programs, and increase assurance that their AML transaction monitoring systems are operating effectively.

An in-depth discussion

Institutions may occasionally address the effectiveness of their AML monitoring systems, but are they looking at the right things?

Many institutions have overlooked the need to periodically review AML monitoring data that is essential for a fully functioning and efficient AML monitoring system. Despite the dramatic increase in transaction volume, mass consolidation of institutions post-financial crisis, ever-expanding product lines, and a continuously shifting regulatory and business landscape, many institutions still base their AML decisions on source data classifications and mappings established by their initial assessments, which may have been performed eight to 10 years ago.

This reliance on an initial data assessment can have an adverse impact on the effectiveness of an institution's AML compliance program. Consider an institution that, prior to the financial crisis, was a typical deposit and loan regional bank. When its AML monitoring system was implemented, the appropriate compliance and technology personnel worked with each business line to identify all of the bank's products and transaction types that required AML monitoring. Every system and data source was evaluated, and the relevant underlying data was mapped to the AML monitoring system's transaction codes so that the monitoring rules could help identify potentially suspicious transaction patterns.

Fast forward to today: Since its initial AML monitoring system implementation, this bank not only acquired and integrated two institutions, but it also transformed its commercial lending function by implementing a new servicing system, expanding its product offerings and revamping its online banking function. With each of these institutional changes, a complete reassessment of the AML transaction monitoring system's reference data and transaction code mappings should have been performed in conjunction with the business lines, compliance, and IT. This reassessment did not occur, however. Instead, the institution spent time and money performing a complete AML transaction monitoring rules optimization project with the intention of generating more productive alerts with less false positives. Because there was no reassessment of the reference and transaction data, the institution used inaccurate and incomplete data as part of its rules optimization process. Unfortunately, during a regulatory examination focused on the optimization changes to the rules engine, the regulators uncovered several data issues and required the institution to perform a transaction lookback.

Why transaction codes matter

Institutions utilize transaction codes to identify and differentiate financial transactions. These codes are significant to a number of operational processes within institutions, such as the monitoring of transactions for anti-money laundering purposes. Transaction code classification and mappings are used across various AML systems to effectively determine which transactions are in scope for AML transaction monitoring. Additionally, the mappings are used to categorize each transaction into appropriate AML transaction groups, such as cash, wire, monetary instruments, account transfers, etc., which makes monitoring more consistent across business lines and geographies. Effective transaction monitoring and validation have become extremely difficult due to increasing transaction volumes, expanding business lines and geographies, and perpetual changes to the business landscape.

As we see from this example, several risks emerge when an institution overlooks the need to periodically reassess its transaction monitoring reference data, especially when institutions are transforming as rapidly as they are today and need to continuously monitor the reference data for changes. These risks include large monetary remediation penalties from regulators, excess costs in terms of staff hours (time to run exception reports, deal with false positives, etc.), and reduced assurance that the AML program is working effectively. The key to reduce these risks is to focus on upstream data sources and how that data is managed as opposed to analyzing the downstream data elements that comprise an AML monitoring system's alert engines. A solution that pairs transaction reference data management with a reconciliation utility is crucial to maintaining acceptable levels of data quality in monitoring systems. It can enable institutions to stay ahead of quality issues and reduce institutional risk.

Diagnosing your transaction data problem

Managing multiple source systems and the massive volume of transaction data these systems can generate is challenging. Determining which codes should be included or excluded, documenting the AML data flow or modification logic, and establishing a consistent, enterprise-wide data integrity standard are a few of the obstacles institutions must successfully hurdle to manage transaction data effectively.

Controls issues

Your institution may be experiencing transaction data control issues if:

- A large number of inactive transaction codes exist.
- Transaction codes in other jurisdictions are not in the language required by home country regulators.
- Incorrect transaction-to-transaction code assignments exist.
- Inconsistencies in transaction code mapping exist.
- A large number of transaction codes are excluded when they should be included.
- A large number of transaction codes are included when they should be excluded.
- Miscellaneous and ambiguous transaction codes represent a large number of transactions.
- Transaction codes are managed differently across business sectors and countries.

Tracking and documentation issues

Your institution may be experiencing transaction data tracking and documentation issues if:

- Little or no documentation exists on transaction code inclusion or exclusion and mapping determinations.
- Little or no documentation of AML data flow and modification logic exists as data travels from source systems to data warehouses to the monitoring system.
- There is no way to prove that transaction volumes in source and monitoring systems reconcile.
- Transactions from a source system are "lost" and not loaded into the monitoring system.
- There is no central organization ultimately responsible for resolving AML data integrity issues and performing active reconciliation reviews, root-cause analysis and correction, and completeness testing.

Data integrity issues

Your institution may be experiencing data integrity issues if:

- Data definitions are inconsistent between functions and typically there is no current enterprise-wide data integrity standard for transaction codes.
- How institutions resolve data integrity issues among their various functions (front office, IT, operations, compliance), business sectors, and geographies is unclear.
- Managing data integrity and reconciliation between the systems and countries is highly complex because of the inconsistencies in how data is handled.
- Often, data completeness and accuracy issues are manifested downstream when the AML monitoring system produces a high number of ineffective alerts, which drives significant costs for little value.
- Data integrity issues are generally discovered when a compliance failure occurs, leading to costly remediation efforts.
- Initiatives address transaction code data for specific purposes, but there is no overarching governance of transaction code integrity.

The right approach—transaction reference data management paired with a reconciliation utility

Data is collected and stored in various systems within the business lines. For example, commercial lending functions typically have an origination system and a servicing system. In some cases, the same information (e.g., customer and account data) is stored in each system and other data points (e.g., customer credit information) is only stored in the origination system.

Data about a customer may reside in multiple systems across different business lines. This data is typically manipulated, aggregated, and stored in databases and warehouses between the source systems and the AML surveillance system. This data manipulation is often complex and undocumented, which presents challenges to AML transaction monitoring.

Data is typically manipulated using various types of programming logic in one or more ways as it is prepared to be passed to AML monitoring. It is at this point where failures can occur and go undetected for long periods of time. Types of data manipulation logic include:

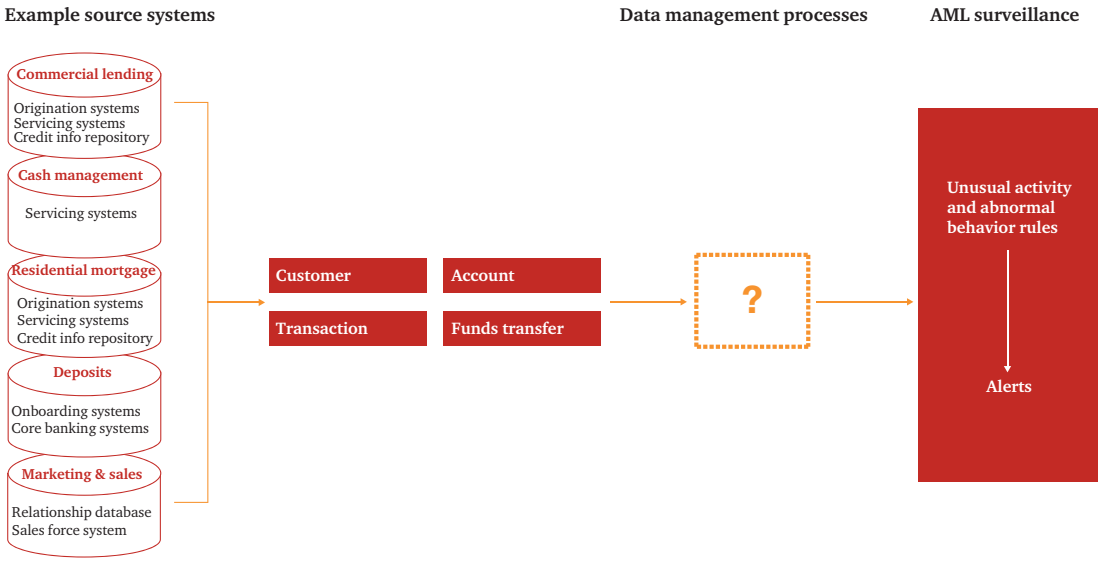
- Transaction code inclusion/ exclusion logic
- Matching logic (e.g., match to value in lookup tables for routing information)
- Text parsing logic
- Currency conversion logic
- Aggregation logic (e.g., aggregating small dollar transactions into one aggregated transaction)
- Reassignment logic (e.g., reassignment of a group of transactions to another transaction code)
- Transaction filter logic (e.g., exclusion of reversals)
- Data enrichment logic (e.g., augmenting with party details)
- Field exclusion logic (e.g., field not carried through from source to monitoring system)
- Multiple transaction legs handling (e.g., transaction description field exceeds maximum text field capacity so additional transaction legs are created to handle text overflow)

Issues that can arise from errors in the data manipulation process include:

- Defect in data manipulation process results in $0 currency conversion issue that goes unde-tected because $0 is ignored by monitoring system rule.
- Certain alert rule required fields (e.g., beneficiary name) are not populated and 99% of input transactions are subsequently ignored by monitoring system rule.
- New funds transfer transaction code is created and not classified as either included or excluded in monitoring. Process does not know how to handle so defaults to excluded. All related transactions never reach monitoring system.
- Process enriches null address field with default value. This results in a high number of false positives generated for certain alert rules because address is used as a point of aggregation.
- Process treats certain electronic funds transfers as SWIFT wires and parses identifier field as if it were a BIC code which erroneously pulls two digit characters and treats them as country codes. This leads to the generation of a high number of alerts to high-risk countries.
- Process treats each leg on a transaction as a transaction resulting in a large number of duplicate entries.

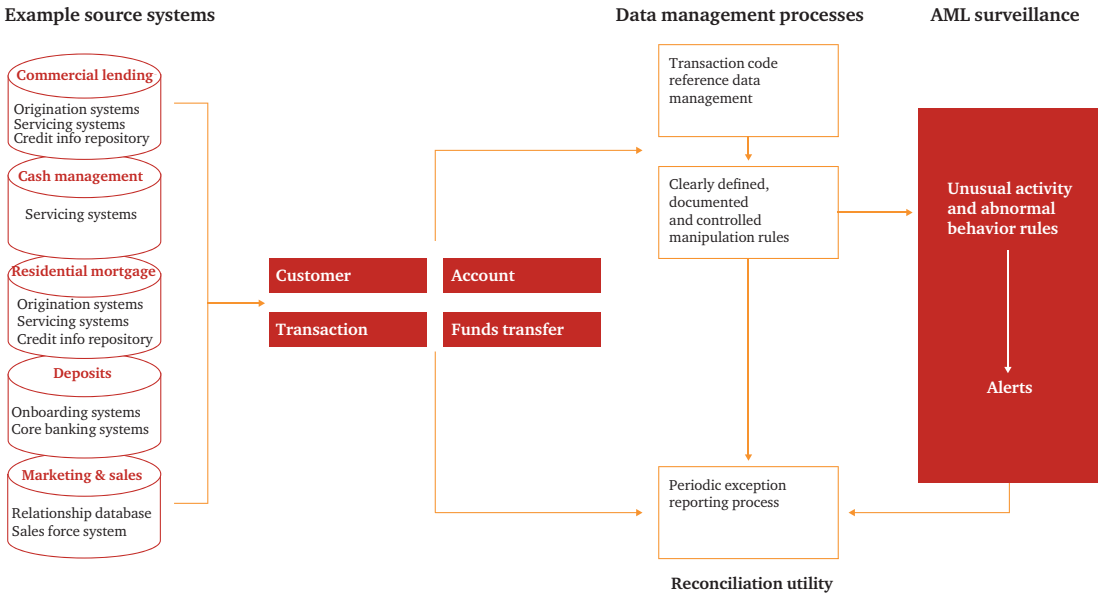
As AML requisite data moves through the data process flow from source to surveillance, it is manipulated, treated, and transformed one or more times. What exactly is occurring to the data and how does this impact the ability to effectively monitor that data?

Figure 1



A controlled system ensures that transaction codes in scope for monitoring are properly managed, that a compliance review was performed and that IT implemented the change correctly. The transaction reconciliation utility provides exception reports to evidence effective system transaction flow. By addressing the quality and consistency of transaction code data, institutions can save time and money, avoid substantial fines and costly remediation programs, and increase assurance that their AML transaction monitoring systems are operating effectively.

Figure 2



How data quality affects AML transaction monitoring

The accuracy and completeness of data can have a significant effect on the quality of the alerts generated by a transaction monitoring system. Often, streams of data are manually and electronically transformed multiple times from source systems on their way to becoming imported into an AML surveillance system. These transformations can generate conversion errors that may lead to incorrect alerts or even result in high-risk information failing to trigger an alert.

Further scrutiny of how transaction data flows through an AML system demonstrates why institutions should go beyond analyzing their downstream data elements. In this hypothetical example, suppose 1 million wire transactions are fed into an AML alert engine and 1,000 alerts are generated (for simplicity's sake, assume one alert contains only one transaction). Of these 1,000 alerts, 50 require a suspicious activity report (SAR) filing. One might conclude that this alert rule is well-tuned given its 1-to-1,000 alert-to-transactions rate and 5 percent SAR filing rate.

However, closer inspection of the 1 million wire transactions reveals that the amount field for 900,000 of the transactions is $0. Why would 90 percent of the transactions have a $0 amount? A root-cause analysis identifies an issue with the transformation of wire transactions from source system to AML alert engine. Non-US currency transactions that need to be set to US currency are erroneously set to $0 because there is an error in the spot-rate conversion logic.

How does this affect optimization results? Since the alert rule ignores all amount values of $0 or less, the effect is substantial. Essentially, the alert engine bypassed 90 percent of the transaction data. Because of this inordinate number of unevaluated transactions, a time-consuming, expensive lookback is required. The critical takeaway from this example is that simply looking at transaction counts of rule inputs and outputs for threshold analysis, without first validating that the underlying data is aligned with the data requirements of the rule, can lead to incorrect conclusions and costly consequences.

Establishing a transaction reference data management system

Assessing the accuracy and completeness of a financial institution's data at the root of its source systems is far from a simple task. The complexity and sheer number of variables that affect institutions' attempts to enhance their transaction data and systems make it essential to consider a more far-reaching solution than simply tweaking their alert engine monitoring rules. This solution begins with the implementation of a system of comprehensive transaction reference data management, and it supplements the system with a reconciliation utility that provides reports that evidence effective system transaction flow.

There are four main components to establishing a transaction reference data management system:

- Establish a baseline
- Policies and procedures
- Classification and assessment
- Monitoring and validation

Establish a baseline

Establishing an enterprise-wide transaction code treatment process within the AML compliance organization is a critical first step in the implementation process. For many institutions, little or no documentation exists that details how mapping is determined or when transaction codes should be included or excluded from consideration in an AML transaction monitoring system. By documenting the rationale and process for including or excluding transaction data as it flows from the source systems to monitoring systems, a quality baseline is created for existing transaction codes.

Policies and procedures

While the baseline step helps explain why transaction codes may fall within AML monitoring parameters, creating the policies and procedures for how transactions codes are created, modified, and managed lays the groundwork for an institution to establish a uniform, enterprise-wide process for handling transaction code data. This step is where buy-in from all functional stakeholders is a must. It can help institutions avoid problems such as front-office personnel not properly implementing changes suggested by back-office compliance teams, or the business approving a code strategy before compliance has a chance to review and assess it.

Making compliance a stakeholder in the transaction code management process offers back-office teams insights on strategic business decisions and allows them to participate in the process of creating or amending the transaction codes that support these decisions. The front office also plays an integral role in the transaction code compliance process. Proper training on the importance of standardized transaction codes and transparent communication from management on why these policies and procedures must be followed, as well as how business objectives will be achieved as a result, will help the front office ensure that changes are implemented as planned.

Classification and assessment

With a transaction code treatment process and the policies and procedures surrounding how to create, modify, or delete transaction codes in place, an institution needs to develop a process for classifying and assessing new or modified transaction codes and determining if these codes should be included or excluded from the AML surveillance system. This process will help an institution overcome problems related to time—when the business needs immediate execution for a new product, for example—and the decentralized and manual management of transaction code lists, which can be more costly and prone to errors than a centralized, automated classification system.

To address timing considerations, an institution can establish a "blanket" documentation process and use preapproved compliance assessments to meet its business needs. On the cost front, there are many ways an institution can leverage a centralized transaction code administration process. When differences are not warranted, it can limit the number of unique transaction codes managed by the institution through standardization of transaction codes. A centralized system can also automate notifications of new or amended transaction codes to compliance, produce and manage a centralized list of all transaction codes across an institution, and develop a systematic approach to reporting all new transaction codes and their corresponding compliance and business assessments.

Another way to help mitigate costs when changes to transaction codes need to be implemented is to design the transaction code assessment process as a middle-office hub. This function would include the periodic reconciliation of the transaction codes within each source system to a standardized master list of transaction codes. The design will help limit the costs and risks associated with the implementation of controls within each product processor.

Monitoring and validation

The final component to an effective transaction reference data management system is to validate that transaction codes are monitored completely and accurately, including activity within inactive codes. Once this stage is reached, the automated system and the compliance officers who oversee it will periodically assess whether new or modified transaction codes' status should be reclassified as in scope or out of scope.

Developing an effective reconciliation utility

Once the transaction reference data management system is in place, a dedicated reconciliation utility will help ensure that an institution's AML transaction monitoring system is operating effectively. Establishing and implementing this reconciliation utility typically involves four steps:

- Configuration
- Sourcing and standardization
- Monitoring and event identification
- Exception reporting and response

Configuration

Establish a centralized AML data integrity and reconciliation utility. Ideally, the utility should be housed within a current reconciliation utility already existing within the institution.

Most institutions have a shared service function in place to perform reconciliations for financial reporting processes. Institutions can more rapidly and cost-efficiently operationalize the utility by leveraging the function for AML reporting processes.

Sourcing and standardization

At this stage, the objective is to source and standardize the input and output of transactions from source systems to data warehouses to AML monitoring platforms. An institution should create a standard data model based on the data requirements found within each monitoring system. In other words, the model should be created based on the data that each monitoring rule requires to run efficiently.

Monitoring and event identification

After sourcing and standardization are complete, an institution should monitor and reconcile the inputs and outputs of its transactions as they flow through its systems to ascertain "breaks" in data integrity. This is not as simple as reconciling counts by transaction code given that transaction data is manipulated and potentially changed through its journey to monitoring system. This step will be exponentially more difficult based on the number of transaction processing systems, data warehouses, and AML monitoring systems that an institution operates. Typically, many of the data process rules are embedded within programming code in mainframes and data sourcing tools. Programming code analysis can derive what is happening to required data as it treated by the code. Using the data model created during the sourcing and standardization step, each data point should be traced backward from monitoring system to source system to determine how it is treated. Common treatment includes matching logic (e.g., match to value in lookup tables for routing information), text parsing logic, currency conversion log, and aggregation logic. Given the complexity involved in this step, it should be implemented iteratively so that each proposed release can be proven successful prior to releasing to additional areas.

Exception reporting and response

Once the data treatment process is clearly documented, this information can be built in the reconciliation utility. This will allow exceptions to be generated by the utility rather than by manual review on reconciliation reports. When "breaks" in data integrity are identified, the utility will work with appropriate stakeholders to remediate the root cause and test to ensure the correction was done properly and is functioning appropriately.

Many factors affect the development of an effective transaction reconciliation utility. Some leading practices that broadly apply across all types and sizes of financial institutions include:

- Leverage existing operations and technology when possible.
- Use a risk-based approach to determine appropriate level of monitoring (i.e., at all data process gates or just at source and endpoint).
- Assign ownership of transaction codes so, if exceptions occur, there is accountability of resolution.
- Establish service level agreements to set expectations of unit.
- Use phased implementation that includes pilots with both an easy, quick win and a complex area.
- Report usability is a key factor to long-term success of reconciliation utilities.
- Reports should highlight red flags and be distributed only to limited numbers of recipients prior to exception confirmation.
- There must be a common set of metrics, but deviation thresholds need to be tailored to risk tolerance of the institution, region, and line of business.
- Control totals and counts are important, but data quality is equally important and must be monitored as well.
- One technology and operations model does not fit all processes from simple to complex.
- Vendor selection is vital. Pick a vendor that offers solutions that are flexible enough to meet your institution's needs. Often premium applications are too complex for simple needs, and simple applications cannot handle complex needs.

Laying the groundwork for an effective solution

Once an institution commits to implementing a transaction reference data management and transaction reconciliation utility solution, there are several steps that will lay the groundwork for a more successful implementation process. Following these steps will help establish buy-in from management and all functional stakeholders. Prior to initiating this type of project, PwC recommends financial institutions:

1. Assemble stakeholders to review current state of AML data control and the effort associated with establishing a common transaction code nomenclature and reconciliation utility and the value to be derived.
2. Develop transaction code reference data and reconciliation utility target operating models (TOMs) (e.g., oversight/standard setting vs. execution of the operational processes).
3. Develop business cases that will contain the investment needed to reach the TOMs and the recommended yearly funding for the effort.
4. Develop a roadmap that prioritizes the effort of the implementation of the TOMs.
5. Establish a steering committee and governance to ratify the initiation of the review, ensure the review is prioritized correctly, and endorse the strategy and business case.

What this means for your business

Institutions reap compliance, financial rewards from solution that combines transaction reference data management with a transaction reconciliation utility

When the most reliable component to the AML compliance equation is change, institutions need to implement a solution that not only periodically validates the quality of its transaction data, but helps institute a framework by which the everyday process becomes an ingrained part of the way the institution conducts its business. By following PwC's approach of managing transaction reference data and implementing a transaction reconciliation utility, institutions can more effectively and efficiently begin realizing the benefits of an enhanced AML monitoring system.

The primary benefits to implementing a transaction reference data management and reconciliation utility solution include:

- Avoiding regulatory remediation (e.g., AML transaction lookbacks)
- Trimming costs by reducing the time and cost per alert of false positives
- Gaining a greater level of assurance that AML systems are accurately capturing the right surveillance data

Before implementation, however, input and buy-in from stakeholders should be secured. The stakeholder groups—compliance, internal audit, IT and operations, front-office business lines—often have different or even competing viewpoints, goals, and motivations for why they would want to manage transaction code data more effectively.

From the compliance team's perspective, implementing this type of solution enhances the team's ability to meet its transparency and completeness monitoring objectives. It also helps compliance quickly and concisely demonstrate the effectiveness of the transaction monitoring processes and systems to regulators and internal audit.

The reconciliation utility can significantly enhance the internal audit process. Instead of internal audit spending the bulk of its time tracing the numbers and verifying the data, the utility can do that work and save time and money by streamlining internal audit's efforts

For the IT and operations group, the solution allows team members to enhance the quality of information and refocus on using automation and analytics to solve business problems. It reduces the number of distinct transaction codes, reduces the number of manual processes, improves the content and integrity of data, and enhances an institution's ability to implement enterprise-wide changes.

The last thing front-office personnel want is for compliance to hinder their ability to do business.

Effective transaction reference data management and the reconciliation utility provide several top-line benefits. They help improve customer service standards, enhance the ability to leverage data assets to improve existing businesses or enter new markets, and allow the institution to better compete by providing comparative information across customer segments and markets.

Some top-tier institutions have implemented or are in the process of implementing a solution that effectively manages transaction reference data and uses a transaction reconciliation utility. They have significantly impacted their AML monitoring performance as a result of this focus on assessing the upstream data processes. Rather than serving as a strictly back-office compliance function, AML transaction monitoring, when done correctly with accurate and complete data continuously tracked at the source systems, can benefit all areas of an enterprise. The hard and soft benefits matrix (see Figures 3 and 4) helps quickly show the benefits realized by the compliance, IT and operations, and business and front-office teams.

Figure 3: Hard benefits matrix

Benefit	Compliance	IT / Ops	Business / Front Office
• Reduced costs related to the reduction in AML regulatory remediations	●	●	
• Reduced internal costs in dealing with business non-compliance	●	●	
• Reduced IT and business costs associated with maintaining a large number of heterogeneous transaction codes	●	●	●
• Improved breath of revenue channels by broadly releasing region-specific strategies			●
• Increased revenue from more precise and consistent transaction pricing			●
• New revenue channels by monetizing as an asset the aggregate benchmark information of customer activity across the bank			●
• Enhanced ability to cross-sell with transaction code usage as an additional data point in customer segmentation			●

Figure 4: Soft benefits matrix

Benefit	Compliance	IT / Ops	Business / Front Office
• Improved AML oversight within institution by optimizing AML systems	●	●	
• Better alignment of all compliance-related activities that require transaction codes	●		
• Enhanced view from regulators	●		
• Improved analyst productivity and depth and breadth of analysis		●	●
• Improved consistency in reporting across regions and lines of business		●	●
• Improved timeliness of the implementation of cross-region/business unit strategies that require like transaction codes		●	
• Reduced risk from incremental, staged implementation of new AML and other technologies that rely on transaction codes and transactions from product processors		●	
• Improved attractiveness of institutions to customers by making it easier for them to transact across regions and business units by standardizing transaction services and pricing			●

Case study

Challenge

A bank had been making annual adjustments to threshold levels of its alert engines in its anti-money laundering (AML) monitoring system, but data issues had been triggering regulator-mandated lookbacks in recent years. To help resolve these issues, the bank was in the process of launching an initiative to improve its data controls for AML compliance across all businesses and regions globally. By proactively monitoring compliance data control risks, the client anticipated improving its ability to detect and address issues before they become regulatory concerns, while possibly increasing its operational efficiency through fewer false positives. The first step in the improvement process was to assess transaction code reference data for consistency and accuracy prior to its usage in the AML monitoring systems.

PwC's role and objectives

PwC undertook an effort to review all transaction codes for monitoring inclusion or exclusion classification and AML system mapping. PwC identified more than 100,000 transaction codes from 125 core banking systems that required review. PwC applied a mixed approach that included an automated, knowledge-based code description classification; a targeted transaction sampling technique; a transaction existence and flow review; and a controlled manual review using PwC proprietary software.

Value to the client

PwC's approach ensured that the review effort applied risk concepts consistently across the various geographies and businesses while allowing for the inherent differences that exist within each. It also accelerated the review process in a controlled manner while ensuring accuracy and completeness with minimal impact to IT, operations, and compliance.

The bank was able to eliminate a large amount of unnecessary data that was impacting the alert generation process as a result of PwC's recommendations. The bank also reduced its risk exposure by proactively identifying a small number of transaction codes that should have been included in monitoring. This initiative improved the effectiveness and efficiency of the bank's AML monitoring system and laid the groundwork for creating and implementing a sustainable function for managing transaction code reference data and an AML data reconciliation utility.

Contacts

To have a deeper conversation about how this subject may affect your business, please contact:

Jeff Lavine
Partner
703 918 1379
jeff.lavine@us.pwc.com

Patrick Giacomini
Partner
646 471 4399
patrick.a.giacomini@us.pwc.com

Thomas Messina
646 471 4757
thomas.messina@us.pwc.com

Nathan Thomas
646 471 2199
nathan.thomas@us.pwc.com

Marco Iacono
641 471 4648
marco.p.iacono@us.pwc.com

www.pwc.com/us/banking