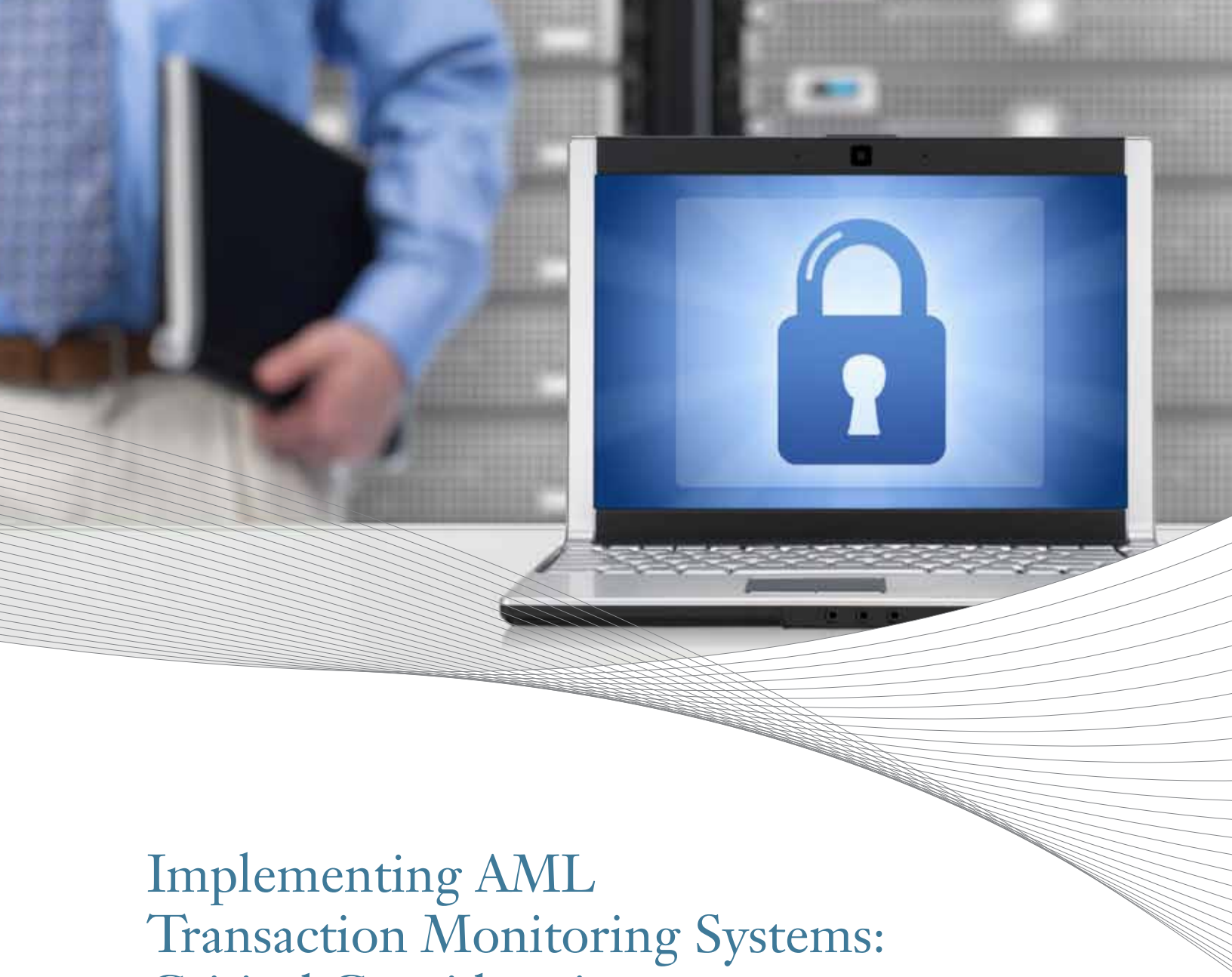

Implementing AML Transaction Monitoring Systems: Critical Considerations

protiviti®
Risk & Business Consulting.
Internal Audit.

Powerful Insights. Proven Delivery.®

ISSUE

From a software implementation perspective, implementing an anti-money laundering (AML) transaction monitoring system may seem no different from implementing any other system; however, there are numerous AML risk factors that an institution should consider during such an implementation. For a successful implementation, institutions should address, among other standard considerations, issues such as identification of risk-based suspicious activity monitoring scenarios, determination of initial thresholds for the identified scenarios, and deployment of the system while integrating it with the institution's technology infrastructure. Improper consideration of these factors could lead to a high number of false positives, increased operational costs, missed reporting deadlines, and, most importantly, undetected suspicious activity and regulatory criticism.

CHALLENGES AND OPPORTUNITIES

In our experience, organizations face multiple challenges with AML transaction monitoring system implementations, including:

- **System Planning:** The planning phase is very important and if not carefully deliberated will result in costly errors, and/or the need for future workarounds or remediation. A critical issue to be considered during this phase is scenario selection based on the institution's AML risk assessment, customers and products. In addition, data source systems will need to be identified and data extraction processes developed.
- **Implementation:** The implementation phase poses numerous challenges and requires the financial institution to have a disciplined approach to various aspects of project planning, effective coordination among various stakeholders of the project, and an overall oversight of the system implementation from a project management office (PMO) level.
- **Initial Threshold-Setting and Tuning:** The threshold values driving each of the selected scenarios should be set at a risk-responsive level to ensure the institution is alerting on potential suspicious activity. At the same time, the institution should be mindful of not setting the threshold values too low, which can result in a high volume of false positive alerts that create operational bottlenecks.

Despite these challenges, a disciplined system implementation approach yields opportunities and favorable outcomes, including:

- **Implementing Risk-Focused Scenarios:** By executing a systematic scenario selection process, the financial institution is able to select targeted scenarios tailored to the institution's AML risk profile. Implementing appropriate risk-based scenarios can improve the efficiency of the financial institution's compliance personnel.

- **Deeper Understanding of Source Data and Coverage:** AML implementation projects often uncover data architecture issues with source systems or transaction codes that need to be addressed as part of the project to ensure adequate and accurate data is flowing into the AML transaction monitoring system. As a by-product of this exercise, the implementers will gain in-depth knowledge of data coverage (e.g., products, transactions, accounts) associated with the chosen scenarios and therefore will enable the institution to answer system "metadata"-related questions posed by the regulators in a more confident and precise manner.
- **Ongoing Scenario and Threshold Maintenance Process:** Challenges experienced during the implementation process due to lack of a systematic threshold-setting and tuning process could be used as lessons learned, and allow the institution to develop an ongoing methodology for scenario threshold-setting (limits) and tuning, which can also lend itself to easy validation by the internal audit team.
- **Efficient Deployment Process:** The existence of a PMO promotes clear coordination among various teams responsible for a flawless deployment of the monitoring system. This coordination will enable the project's key stakeholders to gain a clear understanding of the project state and react in a timely manner to make the required changes.

OUR POINT OF VIEW

Significant effort is needed to achieve an effective AML transaction monitoring system implementation. Based on our past experiences, we have identified some of the most important considerations that should be addressed to successfully implement a technology-driven transaction monitoring system.

SYSTEM PLANNING

Understanding Risks and Potential Red Flags: This task involves effectively mapping the risks identified in the institution's AML risk assessment and common money laundering red flags (i.e., "Money Laundering and Terrorist Financing Red Flags" included in the *FFIEC BSA/AML Examination Manual*) for the respective lines of business with current transaction monitoring controls. Mapping these will be the first step in identifying potential gaps in the current monitoring controls and the scenarios that are necessary to ensure adequate coverage of products/services, and mitigation of money laundering risks.

Vendor Selection: To perform effective vendor selection, the following points should be considered:

- **Data Volume:** Will the chosen product be able to manage the data volume imposed on it? Failure to perform this analysis can result in significant performance bottlenecks.
- **Technology Infrastructure:** Given the significant operational costs associated with the deployment and maintenance of a monitoring solution, will the selected solution be able to coexist seamlessly in the existing technology infrastructure?
- **Scenario Selection:** Does the vendor's solution offer the correct coverage of red flag detection scenarios to meet the institution's risk tolerance and ensure all products and services are adequately monitored? Similarly, does the vendor's system allow for easy customization if it does not offer all scenarios desired by the institution? As a general rule, the more complex the activities of an institution, the more likely customization will be required. Failure to pose such questions up front could drive the need for costly workarounds later or additional development time to program such scenarios. It is also imperative to note that not all vendor-developed rules or scenarios may be required to be deployed by the institution, as the risk exposure for each institution is different and the scenario selection should be performed on a case-by-case basis.

Data Source Identification: From a technology perspective, this task involves identification of various source systems which house the required data. It also involves determining processes that will be responsible for extraction and loading of the data into the chosen monitoring system. The implementers can then create a "dictionary" (metadata) of data sources, and determine which products/transactions should be in scope for monitoring.

The following items are key points to note for data sourcing:

- **Data Availability:** Is the in-scope data readily available?
- **Data Quality:** Has the validity of the data quality been verified? This is a critical step, as inaccurate information (e.g., miscoded transactions) can lead to skewed data analysis and undesired/inaccurate results. For example, when designing scenarios to capture wires flowing to high-risk jurisdictions, it is imperative that the data elements containing all the countries through which the wire was routed are present, and that country codes/values are accurate.
- **Data Refresh Rate:** How often is the data refreshed?
- **Data Volume:** Has data analysis been performed to determine data volume? The data volume should be supportable by existing hardware infrastructure either "as-is" or additional hardware resources should be procured.

Scenario Development: This task involves translating each monitoring scenario's functional specifications into a deployable module based on the chosen transaction monitoring system. Typically, this task is executed by the vendor of the monitoring system, but the institution may choose to design code and test the scenarios itself. In addition, the institution may desire customized scenarios to adequately cover money laundering risks specific to the institution itself.

IMPLEMENTATION (PMO)

Project Planning: This task requires the creation of project plans by taking into consideration the people, resource constraints and effort required to implement the chosen scenarios. This may encompass the creation of a multiphase deployment plan, which will require placing multiple deployments into production in a phased manner.

Resource/Financial Management: This task requires understanding and effectively managing the constraints arising due to people and process resources. Additionally, the time and money spent due to the current project is closely tracked such that any issues arising are communicated to key stakeholders in a timely manner.

Change Management: During the course of the implementation cycle, there are multiple instances where there may be a need to modify the functional, technical or business requirements. To manage this change effectively and ensure that the appropriate functionality is deployed in production, there is need for a disciplined change management process that focuses on managing the change requests, procuring required approval from key stakeholders, and maintaining an open communication channel among all responsible parties. Additionally, this task involves working with the technology deployment team to transition the system into the production environment effectively.

THRESHOLD-SETTING/TUNING

Customer Segmentation: This task involves applying various data analysis techniques to the in-scope data to determine the number and type of the customer segments that can be deployed in the system. Successful execution of this step enables the implementation team to determine appropriate thresholds based on the behavior exhibited by the respective customer segment, as opposed to a threshold gauged on the entire customer base.

Initial Threshold-Setting: In this step, advanced statistical analysis is used to determine effective threshold values which should be applied to a given scenario for successful execution. The threshold-setting exercise should be performed for each customer segment and risk level. Therefore, it is possible to have multiple threshold values for a given scenario, as each value will be applicable at a given customer segment and risk level.

Threshold-Tuning: Prior to going live with the chosen thresholds from the initial threshold-setting exercise, a dry run of the alert-generation cycle should be performed to produce alerts that can be investigated in the test environment. A successful investigation of these alerts can provide insight into the alert quality to be expected in the production environment. Therefore, this step gives an opportunity to perform further threshold-tuning before deploying the selected thresholds in production.

Ongoing Tuning and Threshold Enhancements: Additionally, it is imperative to execute a threshold-tuning exercise on a periodic basis that consists of generating and investigating alerts just below the threshold values. This exercise gives insight into the existence (or lack) of suspicious activity just below the set thresholds. Existence of such activity will require the thresholds to be lowered. If there is no suspicious activity just below the threshold values, then a separate exercise consisting of lifting the threshold values above the current values can be performed. If this exercise yields the same alerts, then there may be a case for lifting the threshold values in production.

HOW WE HELP COMPANIES SUCCEED

Our Risk and Compliance professionals focusing on AML Technology[1] can help your institution implement and maintain a sound and robust AML transaction monitoring system and facilitate a smooth transition to the technology support team at your institution. Collectively, we have full life cycle transaction monitoring system implementation experience and have helped clients deploy and tune AML transaction monitoring systems on various platforms such as, but not limited to, Actimize, Detica NetReveal AML (Norkom), Mantas and SAS AML, as well as a number of homegrown systems, and can therefore help you in any or all of the following service areas:

- Understanding AML risk and assisting the implementation team in ensuring adequate coverage of products/services, transaction types and customer types from a monitoring perspective
- Reviewing and analyzing the available data sources to determine the processes responsible for data extraction and successful loading of it for further downstream processing
- Providing transaction monitoring scenario design and development insight from a technology perspective coupled with AML subject-matter expertise
- Analyzing the existing customer base and its transactional activity to segment customers to enable effective threshold-setting of the selected scenarios

[1] Protiviti plans to address key issues by publishing an AML series in 2013, which will be available later in the year at: www.protiviti.com/AML.

- Performing in-depth statistical analyses to identify initial threshold values, based on customer segment and the risk level exhibited by the customer
- Revising/tuning the initial threshold values by reviewing existing alert quality and executing relevant data analyses to improve future alert quality
- Providing PMO oversight that includes project planning, project coordination, resource and financials management, and change management expertise; we leverage not only our AML technology insights, but also our software implementation experience gathered through successful execution of various IT projects
- Developing both a methodology and approach that will allow institutions to repeat the process by addressing the points identified above on an ongoing basis, and formally documenting those actions such that they can be shared with regulators to exhibit the performance of due diligence

EXAMPLES

Example 1

A large global bank sought our assistance in complying with the terms of its regulators following an independent review related to enhancing its current AML transaction monitoring systems. As part of the project, the global bank also sought our assistance in implementing a new transaction monitoring system for its capital markets division, as well as tuning existing systems for its retail, private banking, and wealth services divisions.

Together with the bank, we developed a strategy and implemented a methodology for initially and continuously assessing the institution's risk; identifying source systems and transaction codes; ensuring accurate data feeds; selecting scenarios aligned with the institution's risks; performing quantitative analysis to calibrate the systems; using the analysis and available "know your customer" (KYC) data to segment the customer base in a meaningful manner; and testing the output and effectiveness of the generated alerts to drive further recalibration of the thresholds and scenarios. Through our efforts, the bank was able to demonstrate to its regulators that it was taking corrective action in implementing strong AML controls in relation to its transaction monitoring systems.

Example 2

A large financial services company sought our assistance in implementing a new AML transaction monitoring system for monitoring its capital markets and brokerage services. We provided both PMO and AML subject-matter expertise.

We developed a strategy and implemented a methodology for initially and continuously assessing the institution's risks; identifying source systems and transaction codes; ensuring accurate data feeds; selecting scenarios aligned with the institution's risks; performing quantitative analysis to calibrate the systems; using the analysis and available KYC data to segment the customer base in a meaningful manner; and testing the output and effectiveness of the generated alerts to drive further recalibration of the thresholds and scenarios. Through our efforts, the financial services company was able to demonstrate to its regulators that it had proactively enhanced its controls and effectively moved toward a more mature and sophisticated transaction monitoring solution to mitigate its money laundering risk.

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. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE® 1000 and Global 500 companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half International Inc. (NYSE: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

Contacts

Carol Beaumier
Managing Director
+1.212.603.8337
carol.beaumier@protiviti.com

Luis Canelon
Senior Manager
+44.20.7024.7509
luis.canelon@protiviti.co.uk

Andrew Clinton
Managing Director
+44.20.7024.7570
andrew.clinton@protiviti.co.uk

Carl Hatfield
Director
+1.617.330.4813
carl.hatfield@protiviti.com

Bernadine Reese
Managing Director
+44.20.7024.7589
bernadine.reese@protiviti.co.uk

Chetan Shah
Associate Director
+1.704.972.9607
chetan.shah@protiviti.com

THE AMERICAS

United States

Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Denver
Fort Lauderdale
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Woodbridge

Argentina
Buenos Aires*

Brazil
Rio de Janeiro*
São Paulo*

Canada
Kitchener-Waterloo
Toronto

Chile
Santiago*

Mexico
Mexico City*
Monterrey*

Peru
Lima*

Venezuela
Caracas*

EUROPE

France
Paris

Germany
Frankfurt
Munich

Italy
Milan
Rome
Turin

The Netherlands
Amsterdam

United Kingdom
London

MIDDLE EAST

Bahrain
Manama*

Kuwait
Kuwait City*

Oman
Muscat*

United Arab Emirates
Abu Dhabi*
Dubai*

ASIA-PACIFIC

Australia
Brisbane
Canberra
Melbourne
Perth
Sydney

China
Beijing
Hong Kong
Shanghai
Shenzhen

India
Bangalore
Mumbai
New Delhi

Indonesia
Jakarta**

Japan
Osaka
Tokyo

Singapore
Singapore

South Korea
Seoul

* Protiviti Member Firm
** Protiviti Alliance Member

protiviti®
Risk & Business Consulting.
Internal Audit.