Views on AML Technology

Volume II

Validation, Selection, Metrics and More
Table of Contents

Introduction ................................................................................................................................................. ii

Sanctions Screening Systems: “Plug and Play” Is a Thing of the Past ......................................................... 1

Validating Real-Time Sanctions Screening Systems: Critical Considerations ............................................. 5

Improve Threshold Values Tuning of Transaction Monitoring Systems by Taking a Qualitative Approach .................................................................................................................................................. 9

Measuring the Right Metrics and Leveraging Risk and Performance Indicators to Enhance the End-to-End Transaction Monitoring Program ................................................................................................... 12

Internal Audit’s Expanded Role in Assessing AML Technology .................................................................... 17

Examples of Protiviti’s Work With AML Transaction Monitoring Systems .................................................. 20
Introduction

One of the key challenges to maintaining an effective anti-money laundering compliance program remains the effective use of enabling technology. In Protiviti’s Views on AML Technology, Volume II, we explore:

- The selection and validation of sanctions screening systems
- The advantages of a qualitative approach to threshold setting for transaction monitoring systems
- The use of key performance indicators and key risk indicators to enhance the transaction monitoring program
- Internal audit’s role in assessing AML technology

This publication is a compilation of point-of-view (POV) papers that we published throughout 2014.

We hope this information will be of interest and help to you. We would welcome the opportunity to speak with you about your organization’s specific needs regarding AML and sanctions screening systems and about AML compliance in general. Our team includes highly experienced AML and sanctions subject-matter experts as well as specialists in AML technology and Ph.D.-level professionals with deep quantitative and analytical skills. For your convenience, a list of Protiviti contacts is included at the end of this publication.

For copies of other AML- and sanctions-related thought leadership, including Protiviti’s Guide to U.S. Anti-Money Laundering Requirements: Frequently Asked Questions (Sixth Edition), please visit us at www.protiviti.com/AML.

Protiviti
November 2014
Sanctions Screening Systems: “Plug-and-Play” Is a Thing of the Past

Issue

Institutions with deficiencies in their Office of Foreign Assets Control (OFAC) compliance programs and/or violations of the OFAC requirements and other global sanctions programs are increasingly in the crosshairs of regulatory enforcement actions. While poorly chosen or configured sanctions screening technology has not been the root cause of all of the financial services industry’s sanctions problems, it is often a contributing factor. This is leading many financial institutions to abandon manual sanctions compliance efforts and various inefficient “home-grown” and first-generation sanctions screening systems in favor of more sophisticated technologies.

Financial institutions evaluating new sanctions screening technologies on the market should keep in mind that technologies with apparent “plug-and-play” capabilities and promising out-of-the-box functionality are, without question, not the right approach to meeting the expectations of regulators. While a touted plug-and-play, “set-it-and-forget-it” approach sounds appealing, institutions that fail to customize their sanctions screening software will see increased costs and operational risks (e.g., additional personnel to clear excessive false positives) and a higher risk of noncompliance.

Challenges and Opportunities

In our experience, the challenges of implementing a new sanctions screening system and enhancing an “out-of-the-box” one are similar. These challenges have less to do with the technology aspects of implementation (e.g., hardware, user interface design, etc.) and more to do with the complexities of matching functionalities and processes needed to calibrate the technology to the risk profile of the institution. Some of the most common and critical challenges to ensuring maximum effectiveness and efficiency from sanctions screening systems are detailed below:

- **Assessing the adequacy of system functionality.** A vendor solution may offer a set of advanced matching algorithms, which the institution may conclude to be comprehensive without taking into consideration the ethnic diversity of its customer base, potential misspelling of names when accounts are established, special characters (e.g., vowel and diacritic representations, non-standard word splitting, concatenation), etc.
- **Determining sanctions lists.** A vendor solution may include the option of using multiple sanctions lists, e.g., country-specific lists in addition to OFAC, United Nations sanctions, etc. Many institutions rely on these vendor-suggested lists, finding it too difficult to understand or decide which lists actually apply. The result may be unnecessary screening of superfluous lists, which the institution may not be required to scan its customers against, or, conversely, increased risk that the institution has not captured all required sanctions.
• **Consolidating watch list names.** When institutions use multiple lists, there is a high probability that the same entity will appear on more than one list. This can result in multiple, unnecessary hits against the same name and the need to resolve each duplicate hit, unless names are consolidated across the multiple lists used.

• **Identifying adequate matching rules.** Out-of-the-box configurations are often limited to matching entity names against the respective watch list names. The watch lists often contain additional attributes (e.g., date of birth, identification number, country of citizenship, etc.) that can be leveraged for identifying potential hits in a more effective manner (i.e., reduce the number of potential matches generated by applying the additional attributes against customer information, as part of the matching criteria).

• **Determining threshold settings using a systematic approach.** Matching rules generate hits when the score of matching criteria exceeds the pre-determined threshold value (commonly referred to as a matching score). Financial institutions relying on the out-of-the-box settings frequently experience an excessive volume of false positives, all of which must be reviewed and resolved; or, conversely, the system fails to generate hits, due to incorrect setting of the matching score. Regulators expect sanctions screening processes to be risk-based (i.e., commensurate with an institution’s risk profile), but reliance on out-of-the-box thresholds makes this difficult to support.

• **Lack of complete screening coverage of customers/transactions.** Failure to identify and include all data feeds (e.g., customers from various lines of businesses, types of transactions, etc.) that should be scanned by the sanctions screening system can result in a gap in the sanctions screening program.

• **Use of multiple sanctions screening systems.** More often than not, institutions lacking a centralized sanctions screening strategy end up deploying multiple sanctions screening systems (e.g., different lines of business implementing their own sanctions screening systems). This results in multiple versions of the same watch lists, disparate matching rules and varying threshold values, leading to potentially incomplete and unreliable sanctions screening and possible regulatory compliance issues.

Unfortunately, the challenges of implementing a customized system do not end here. Dealing with the sophistication of the logic of sanctions screening systems requires considerable time to configure, as well as a thorough understanding of the institution’s business operations and risk profile/tolerances. Awareness of these challenges can ensure that an effective, efficient, and appropriately risk-based global sanctions compliance program is developed and can facilitate the ongoing management of the system.

The items below detail some of the specific benefits that can be incurred from implementing a customized system correctly:

• **Increased effectiveness.** Customizing the various sanctions lists, identifying the appropriate matching algorithms, tuning targeted rules parameters and adjusting thresholds to identify potential matches all result in increased system reliability.

• **Increased efficiency.** The increased effectiveness of the system also helps to reduce the volume of obvious false positives. This in turn allows the institution, and alert adjudicators in particular, to focus on sanction hits that are more likely to be true sanction matches. As a result, adjudicators are able to refine investigation techniques, expedite review processes, and ensure time spent investigating potential matches is more meaningful.

• **Enhanced confidence through validation.** By independently validating the vendor-supplied system, the institution can gain confidence that the system is working or identify shortcomings that should be mitigated.

• **Centralized sanctions screening strategy.** By expending efforts to understand business operations, the institution’s risk profile and the data feeds responsible for sourcing customers and transactions, the institution is able to articulate a comprehensive centralized sanctions screening strategy that enables more targeted sanctions screening systems.
Our Point of View

The challenges of managing an effective sanctions screening system, and subsequently, a global sanctions compliance program, are not limited to the output and resolution of potential matches. There are a number of significant considerations across the entire lifecycle of the system that the institution must take into account. These include critical stages like vendor selection, calibration, implementation, ongoing tuning, and enhancement of the adjudication process of potential matches.

Based on our past experience assisting institutions with sanctions system implementations and validations, we have identified some of the most important points to consider for effective management of a sanctions screening system. We have broken down the lifecycle of a sanctions screening system into six phases, and detailed in the subsections below the critical considerations relevant during each phase:

Vendor Selection

In order to perform an effective vendor selection, the following questions should be considered:

- **Data volume.** Will the chosen product be able to manage the anticipated data volume? Failure to perform this analysis can result in significant performance bottlenecks.

- **Technology infrastructure.** Given the significant operational cost associated with the deployment and maintenance of a sanctions screening solution, will the selected solution be able to coexist seamlessly in the existing technology infrastructure?

- **Matching algorithm library.** Does the vendor’s solution provide capability to perform matching for non-English names? Does it provide the capability to perform fuzzy matching, and which algorithms (e.g., Levenshtein, SoundEx) are supported by the solution?

Watch List Sourcing

In the initial implementation, this phase addresses the selection of watch lists (both public and internal to the institution) to be used in screening, and the processes necessary to source the chosen lists. As part of ongoing system management, this phase determines the processes used to ensure watch lists are updated timely, accurately and completely.

Matching Rules Identification

Managing a sanctions screening system includes understanding whether an institution’s various processes (e.g., customer onboarding, alert adjudication) can facilitate or support more refined matching rules. More often than not, the institution uses name-only matching rules in the screening system. Since there are additional attributes available both on the watch list and in the customer data, it is imperative that rules are created by employing additional attributes such as date of birth, address, identification numbers, etc., to enable the institution to identify customers who cannot be identified using only a name-matching rule. Additionally, as part of the rule identification process, each rule can be assigned a score to enable investigators to prioritize their workloads.

Workflow Process Identification

The hits generated by the sanctions screening system will need to be investigated; therefore the system must contain an investigation workflow. The workflow should be identified and implemented into the system such that the hits can be investigated according to the business workflow of the institution and the relevant audit trails can be maintained.
Threshold Setting and Tuning

In this step, advanced statistical analyses are used to determine effective threshold values to be applied for each of the identified matching rules for successful execution. Prior to going live with the chosen thresholds from the threshold-setting exercise, a dry run of the matches-generation cycle should be performed to produce matches that can be investigated in the test environment. A successful investigation of these matches can provide insight into the match quality that can be expected in the production environment. This step is important as it provides an opportunity to perform further threshold tuning before deploying the selected thresholds in production.

Screening System Validation

Though this step is not part of the initial implementation phase, institutions, specifically banking organizations, are required to perform an independent validation of the screening system that is currently in production. Below are some tests to consider when performing a validation of the sanctions screening system:

- Extract a statistically valid sample of names from watch lists (Sample 1).
- Extract a sample of names from the institution’s customer base (Sample 2).
- Create variations of sampled names by employing various algorithms like SoundEx, simple permutations, containment, etc.
- Test the system by utilizing a combination of Sample 1 and Sample 2 and their variants.
- Test the system by raising/lowering the matching score threshold values and collect hit statistics.
- Analyze the resulting hits to determine false positive and false negative rates.

The following graphic depicts the phases that constitute the lifecycle of a sanctions screening system:
Validating Real-Time Sanctions Screening Systems: Critical Considerations

Issue

The majority of financial institutions today rely on third-party screening systems to perform sanctions screening. Banking organizations that provide funds transfer services to their customers are under increased scrutiny to perform real-time scanning against various sanctions lists of all payments going out and coming in on behalf of their customers. Similar to the trend we have seen with anti-money laundering (AML) transaction monitoring systems, regulators expect financial institutions to be able to demonstrate that sanctions screening systems are configured correctly. The challenge for financial institutions is finding the right balance between being able to detect sanctions violations and processing payments for their customers without unnecessary delay.

To meet this challenge, it is important that financial institutions understand their screening environments better and comprehensively validate and tune their sanctions screening systems to make sure that they are effective, efficient and provide the required coverage from a regulatory perspective.

Challenges and Opportunities

Financial institutions are presented with a multitude of challenges when it comes to validating and tuning a third-party sanctions screening system successfully. These include:

• **A large number of transaction types.** Typically, banks in the U.S. use either the Fedwire Funds Service or the Clearing House Interbank Payments System (CHIPS). These are the two primary domestic wholesale payment systems used for interbank funds transfers. For cross-border funds transfers, a messaging infrastructure called Society for Worldwide Interbank Financial Telecommunication, or SWIFT, is used. In addition to customer and bank funds transfers, SWIFT is used to transmit foreign exchange confirmations, debit and credit entry confirmations, statements, collections and documentary credits. These transaction types are defined in more than 100 different formats, each denoting a different transaction type. For example, SWIFT MT1nn is used for customer payments whereas an MT2nn format indicates a financial institution transfer. Each message format has unique placeholders for capturing the various data items applicable to that transaction. Identifying these data fields and mapping them accurately to watch lists can be challenging, given the number of different formats.

• **Misconfigured watch lists.** Banks also struggle with choosing the right watch lists for their real-time transaction screening process. Typical problems are scanning against inapplicable watch lists offered by the third-party vendor, scanning against more lists than necessary, and not scanning against relevant lists. These situations can happen if the bank has failed to perform adequate analysis and configuration during the implementation of the third-party system. Some commonly used sanctions lists include the United Nation’s al-Qaeda sanctions list; the Specially Designated Nationals list issued by the U.S. Office
of Foreign Assets Control (OFAC); the consolidated list of Persons, Groups and Entities Subject to EU Financial Sanctions; and the Financial Sanctions list of HM Treasury (UK). Since many of the national sanctions lists are based on sanctions imposed by the UN, names appearing on UN lists can also appear on the lists issued by the EU, OFAC and HM Treasury. Using these watch lists redundantly can result in unnecessary false positives, which can create additional work for investigators and delay payments. On the flip side, not using all the lists that are mandated may result in false negatives, causing transactions involving sanctioned entities to go undetected.

- **Complex proprietary matching algorithms.** Many third-party systems come bundled with complex name-matching algorithms that are difficult for banks to understand. Typically, these algorithms employ various matching techniques to identify records from two sources – the bank’s systems and the third-party watch list – that contain information about the same entity. These algorithms are often proprietary, and the underlying source code is not available to financial institutions to help them understand the underlying methods. Lack of an in-depth understanding of the system negatively impacts the validation strategy and results in financial institutions performing “black box” testing, which doesn’t accomplish the comprehensive validation required from regulators.

These challenges notwithstanding, a comprehensive validation, testing and tuning process of the sanctions screening system is both necessary and possible, with the following benefits to the financial institution:

- **Meeting regulatory expectations.** Periodic testing and tuning of the sanctions screening system allows financial institutions to determine the level of coverage provided by these systems and demonstrate to regulators that their systems and processes are configured in line with regulatory expectations.

- **Reduction in false positives.** Regular testing and tuning helps reduce the false positives the system generates. This improves the efficiency of the sanctions screening process by reducing the number of potential matches an analyst needs to research, increasing productivity and minimizing the risk of delaying a customer's payment.

- **Maintaining control.** Capturing and reviewing key metrics as part of an ongoing tuning process allows financial institutions to maintain continuous compliance. For example, as a financial institution’s risk profile changes (with the addition of new products and service offerings or with changes in the customer base), the system will be exposed to more and different transactions. By tracking key metrics, such as the “hit” rate (i.e., the number of potential sanction matches), financial institutions can see trends and detect spikes or drops in the hit rate which may be an indicator that the system needs to be retuned or that a data quality issue exists.

**Our Point of View**

Validating and tuning a sanctions screening system that scans real-time transactions is a multistage process requiring significant time and effort. Based on our experience, we have identified the following key steps to this process:

**Performing a data integrity audit.** Most organizations store their data in multiple locations in a variety of formats. In order to perform the required validation, financial institutions must ensure that the sanctions screening system is able to access all these different systems and automatically integrate the data sourced from them. For example, payment transactions typically are sourced from the institution’s in-house payment system, while the watch lists are sourced from external list providers; data anomalies or missing data in either of these sources can negatively impact the results of the testing. Thus, auditing all data and checking it for inconsistencies are crucial prerequisites to the validation process.

**Identifying transaction types to be scanned.** To begin the validation process, financial institutions must identify the various transaction types they use in order to ensure proper coverage for the sanctions screening program. Based on their products and service offerings, financial institutions can use any number of SWIFT message formats to provide transactional services to their customers.
The following table, which is intended to be illustrative and not all-inclusive, lists some of the commonly used messages and the scanning requirements for them.

<table>
<thead>
<tr>
<th>SWIFT Message</th>
<th>Description</th>
<th>Scanning Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>MT0nn</td>
<td>System messages</td>
<td>No</td>
</tr>
<tr>
<td>MT1nn</td>
<td>Customer payments</td>
<td>Yes</td>
</tr>
<tr>
<td>MT2nn</td>
<td>Financial institution transfers</td>
<td>Yes</td>
</tr>
<tr>
<td>MT3nn</td>
<td>Treasury markets</td>
<td>Yes, if used for currency exchange and security trades</td>
</tr>
<tr>
<td>MT4nn</td>
<td>Collection and cash letters</td>
<td>Yes, if used to purchase a monetary instrument</td>
</tr>
<tr>
<td>MT5nn</td>
<td>Securities market</td>
<td>Yes, if used for security trades</td>
</tr>
<tr>
<td>MT6nn</td>
<td>Treasury markets – metals and syndications</td>
<td>Yes, if used for security trades</td>
</tr>
<tr>
<td>MT7nn</td>
<td>Documentary credits and guarantees</td>
<td>Yes, if used for letters of credit</td>
</tr>
<tr>
<td>MT8nn</td>
<td>Traveler’s cheques</td>
<td>Yes</td>
</tr>
<tr>
<td>MT9nn</td>
<td>Cash management and customer status</td>
<td>Yes, if used for a wire transfer</td>
</tr>
</tbody>
</table>

**Identifying and mapping the critical transaction data fields.** The data fields of various formats must be matched accurately to ensure proper validation. Funds transfers present an increased degree of risk for financial institutions due to the number and dollar volume of transactions, the geographic locations of originators and beneficiaries and the fact that not all originators and beneficiaries are bank customers. Typically, international funds transfers are performed using one of the global SWIFT formats (e.g., MT103, MT202), and the domestic funds transfers are performed using the Fedwire format. Regardless of the format of the transaction, the following data fields are critical and need to be mapped accurately for testing:

- Originating party’s name
- Originating party’s country and address lines
- Originating bank
- Originating bank’s country and address lines
- Intermediary banks involved in the transaction (first, second and so on)
- Beneficiary bank
- Beneficiary bank’s country and address lines
- Beneficiary party’s name
- Beneficiary party’s country and address lines

**Selecting test samples.** A watch list sample set consisting of both “good” and “bad” samples needs to be created for various systems and comparisons testing. The “good” sample should consist of names which have a very low probability of reconciling to a regulatory watch list. Typically, these are the financial institution’s actual customers who are known to be low risk. The “bad” sample should consist of a statistical sample of names and/or other supporting fields from all the regulatory watch lists that are in use by the third-party system.

**Applying name-masking algorithms.** The “bad” sample should be further expanded to include several variations of a single name. This is done in order to test the capability of the system to apply “fuzzy logic” to match the altered names against the same entity in the watch list. Some commonly used algorithms include:

- **Soundex.** Soundex is a phonetic algorithm for indexing names by sound, as pronounced in English. The goal is for names that are pronounced similarly to be encoded to the same representation so they can be matched despite differences in spelling. For example, Mary can be matched to Marie, and Carmen can be matched to Carman. The purpose of this test is to verify whether the system is robust enough to recognize a misspelling of a name based on pronunciation.
• **Containment.** The objective of the containment algorithm is to provide only a portion of the name while performing the list matching. For instance, Matthew can be truncated to Matt, Robert to Rob, etc. The purpose of this algorithm is to ensure that the sanctions screening system is able to identify a customer based only on a portion of the name.

• **Extraneous characters.** The purpose of this algorithm is to introduce stray characters into the name and test whether the system is able to bypass these extraneous characters and match the name against entries in the watch list. For example, the system should be able to match ODonnell and O’Donnell.

• **Permutations.** Permutations are achieved using various combinations of first, middle and last name. For example, switching the last and first name while leaving the middle (if applicable) the same is one possible variation. Another one is taking the first initial of the first name and leaving the rest of the name unchanged.

**Tuning.** Tuning is the essential and crucial next step in the validation process. The results from the iterative testing process should be used as an input to the tuning process. A sensitivity analysis should be performed by executing “above-the-line” and “below-the-line” testing. This is done by changing the score thresholds above or below the current settings to arrive at the optimal scoring threshold to which to configure the system – one where an acceptable balance exists between true and false positives.

**Test Environment.** Last but not least, a fully functional test environment is key to any enterprise system testing. Because automated batch processing is the most efficient way to test sanctions screening systems, the test environment should be configured to allow for that. For example, a sample of transactions with Soundex name variations for the originating parties could be grouped into a single batch and executed as one test.
Improve Threshold Values Tuning of Transaction Monitoring Systems by Taking a Qualitative Approach

**Issue**

Central to any transaction monitoring system are the threshold values at which each of the selected transaction monitoring scenarios operates. If set too low, threshold values will result in numerous false positives, requiring analysts to expend considerable time investigating useless alerts. If threshold values are set too high, analysts may fail to detect and report suspicious activity, as required by various regulatory agencies across the globe.

In an effort to optimize threshold values, most financial institutions take an approach to threshold setting and tuning that is focused solely on quantitatively determining, or tuning, the threshold values. This approach enables institutions to determine threshold values that are supported by a statistical or a data-driven analysis, but it fails to factor in the business intelligence that can be gleaned from alert investigations and available suspicious activity report (SAR) data.

**Challenges and Opportunities**

In our experience, financial institutions face multiple challenges with respect to tuning threshold values. The most common and critical of these include:

- **Knowledge of business impacts.** More often than not, threshold setting and tuning is executed by a team with deep quantitative knowledge of various model and statistical techniques, but without a strong understanding of alert investigation and the resulting impacts of lower or higher threshold values.

- **Information availability.** Information that would inform the alert tuning process, such as the ratio of alert-to-SARs and the nature of SARs, is not easily retrievable. For example, SAR data may reside in a separate financial intelligence unit (FIU) and may not be easily accessible to a test environment used for evaluating alerts before they are put into production.

- **Resource availability.** Even though an organization may understand the need to perform alert investigations before deploying threshold values in production, it may not have considered the need for seasoned investigators to collaborate with the quantitative team and perform qualitative analysis of the alerts.

These challenges notwithstanding, combining quantitative and qualitative analysis is the only way to ensure that mathematical results are balanced appropriately with real-world business experience and judgment.
The specific benefits you’ll gain from incorporating a qualitative process include:

- **Reduced false positives.** By executing a scenario tuning cycle that includes qualitative analysis, such as historical information gathered at the investigation level of pre-production alerts, a financial institution will be able to establish more targeted thresholds. Additionally, by considering previously filed SARs, the institution can extract pertinent information about clusters of activity responsible for the suspicious activity. This information can then be leveraged to perform tuning of the threshold values for the patterns of activity that are identified in the SARs.

- **Identification of redundant scenarios.** Additionally, through the review of alert-to-case information and SARs, an institution can identify current rules or scenarios that are not yielding productive alerts, and can use this information to evidence redundant/ineffective scenarios and make a case for retiring them.

**Our Point of View**

Based on our experience assisting institutions with threshold tuning, we have developed a threshold tuning methodology that is deeply rooted in the qualitative analysis of potential alerts. The qualitative analysis phase begins after the initial threshold values have been determined quantitatively. At a high level, the illustration below depicts where the qualitative analysis fits in the overall threshold tuning process:

Following are considerations that are especially important for performing effective qualitative tuning:

**Sandbox Environment**

The organization should create a dedicated sandbox environment where the qualitative tuning exercise can take place. The key requirements of the sandbox environment include:

- **Existence of production data.** The sandbox environment should contain production data and be configured to enable an investigator to obtain a real picture of how the alerts will appear when they are actually deployed in production. Key data points are customer, account, transactions and scenarios.

- **Capability to execute alert generation cycle.** The sandbox environment should provide for the capability to execute multiple alert generation cycles to allow for multiple iterations of alert investigations before the right set of threshold values can be deemed appropriate.
Alert Sampling

Alerts that are generated in the sandbox environment should be sampled for investigation. A statistically valid sample should be extracted from the alert population. If the organization leverages customer segmentation or risk levels, then a stratified sample should be extracted such that alerts are sampled from each of the customer segments or risk levels.

Investigations Lite

This is a key phase of the qualitative tuning. Each of the sampled alerts is reviewed by investigators to determine whether it is productive (high likelihood of SAR filing), unproductive (low likelihood of SAR filing) or erroneous (result of underlying bad data such as duplicate transactions, incorrect country codes, etc.).

In order for investigators to perform their analysis effectively, they need the following information:

- **Customer data.** Investigators should have access to the customer data attributes necessary to understand the customer’s background and business or banking activities. Available data may vary based on customer type (individual, business, financial institution).
  - Name
  - Address
  - Occupation or industry
  - Entity type (partnership, limited liability corporation, corporation, trust, private investment company)
  - Income

- **Account data.** Investigators should have access to the account data necessary to understand the nature of the account, as well as the identities of individuals or entities that have access to, influence over or an interest in the account.
  - Account type
  - Date opened
  - Average account activity
  - Related accounts
  - Authorized signatories
  - Beneficial owners

- **Transaction data.** Investigators should have access to the transaction data necessary to understand the nature of the transactions being reviewed.
  - Minimum of six months prior to period covered by the alerts
  - Originator, beneficiary, and intermediary details (e.g., name, address, account number, financial institution, country)
  - Transaction type (ACH, wire, cash, check, internal transfer, etc.)

- **Prior SARs.** Knowledge of prior SAR filings in relation to the customer or a customer’s account will aid in determining the effectiveness of alerts being reviewed by investigators. Alerts of customers or accounts with previous SAR filings may be viewed as more effective than alerts for customers or accounts with no such previous filings.

- **Prior alerts.** An understanding of prior alerting activity and alert dispositions will aid in understanding the kinds of activity that have been subject to previous review and to assist in determining the effectiveness of alerts being reviewed by investigators. Recurring alerts for repeated, nonsuspicious activity may be viewed as less effective than alerts for different potentially suspicious behaviors.
Measuring the Right Metrics and Leveraging Risk and Performance Indicators to Enhance the End-to-End Transaction Monitoring Program

Issue

Escalating regulatory pressures around anti-money laundering (AML) regulations are driving a paradigm shift in how organizations use technology to support their risk management and assurance activities. Optimization of transaction monitoring (TM) systems and supporting processes has been a hot topic over the last few years, and continues to be the focus of regulators and financial institutions today. A question many institutions ask is “How do we know whether our TM systems and/or processes are optimized or not?” The answer is, by creating and analyzing system-generated reports in order to obtain key metrics about the system, which management can use as indicators of operational effectiveness, data quality and system performance. By using these system-generated metrics, key stakeholders can gain visibility into any bottlenecks in the alerts review process, uncover data quality issues and take steps to address areas that may need immediate attention.

Metrics and metrics reporting not only measure the progress and success of the TM program but provide the foundation for an optimization of the system. By using relevant management information (MI) reports and focusing on areas of underperformance, management can put measures in place to address inefficiencies before they have a detrimental effect on the process and the organization.

Challenges and Opportunities

Financial institutions face multiple challenges with respect to obtaining and leveraging the right metrics from their TM systems. Based on our experience, the following situations are typical:

- **Not knowing what to measure.** Often, institutions don’t know exactly what metrics they need to measure. This typically is a result of not understanding which metrics are used to indicate an ineffective system. To ensure that the right metrics are being utilized, a well-defined AML governance framework must be established, along with clearly articulated metrics that can be used to support the business and meet regulatory requirements.

- **Not understanding the data requirements.** More typically, institutions struggle with identifying and sourcing useful, consumable data. Inconsistent, duplicate or out-of-date data will result in poor quality of information from the measurements. Sometimes, the problem is operational – not knowing how to obtain the data on which to perform measurements. To ensure that the right data is used to perform measurements, institutions should a) perform an analysis to determine the correct data parameters to feed into a metric; b) ensure the defined data is suitable, i.e., available, complete, and accurate; c) determine how often the data is refreshed; and d) understand the volume of data required.
• **Having disparate information management systems.** We often see institutions with databases that are fed information from multiple TM systems, delivering inconsistent output from system to system. These inconsistencies typically stem from information systems having different business requirements; from business rules not being applied consistently to all information management systems; or from a lack of understanding of the data structure, resulting in misinterpretation of the sourced data. More often than not, organizations struggle to identify the root cause of disparate reporting on the same metrics when data is sourced from different repositories. These organizations need to ensure that documents supporting the design of existing architecture, particularly business requirement documents, are clear, available and not written at a level that is too high or difficult to comprehend.

• **Lack of a feedback loop between TM and case management systems.** We also see a number of instances where institutions are unable to get the entire end-to-end picture because the MI reports generated from the TM system are not linked to the end results provided by the case management systems. This also creates issues with feeding vital information from cases resulting in suspicious activity reports and suspicious transaction reports (SARs or STRs) back to the TM system’s alert review and tuning processes. An appropriate governance structure will help identify and extract the correct data for the TM system and link case results back to the system, closing the loop.

• **Managing Competing Requirements.** Another typical problem within organizations is the inability to manage multiple stakeholders and deal with a large number of diverse business requirements. Numerous requests for similar reports can clog the system as it attempts to run multiple queries from the same data. Often, the overload stems from a lack of coordination and/or clarity when requesting information. For example, the information requirements that are passed to analytics teams for the same type of report can differ based on who is requesting the report (e.g., middle management vs. executive management). This can lead to analysts spending much of their time producing multiple MI reports instead of leveraging the information from these reports to provide better information for the business.

• **Lack of clarity around broader organizational goals.** TM initiatives driven by upper management may not always trickle down to middle management. Likewise, initiatives driven by middle management may not always align with the overarching enterprise strategy, resulting in disparate and potentially conflicting strategic initiatives moving forward, complicating operating models and wasting effort.

Once these challenges are overcome, however, institutions can gain a number of opportunities to leverage the right metrics to understand and enhance their TM programs:

• **Detection logic effectiveness and alert volumes.** Armed with the right measurements and information, management will be able to identify underperforming detection models and scenarios (e.g., no alerts or too many alerts generated) or changes in alerts stemming from a shift in business requirements, which could highlight the need for tuning of the TM system.

• **Data accuracy.** Management information report results that are well outside of management’s expectations may alert management to data or technical issues and prompt the institutions to address them.

• **Identification of emerging risks.** Reports that are accurate and based on the right metrics may provide insight into new geographic areas or transaction types that are posing increased risk to the institution.

• **Staff performance and competency level.** By reviewing MI report results, management will be able to gauge better the efficiency and productivity of employees and may be able to ascertain whether processes need enhancement or whether additional training should be provided to the staff charged with reviewing the alerts.
Our Point of View

Obtaining the right metrics can provide institutions with information about a number of key risk and performance indicators (KRIs and KPIs) used to gain insight into the effectiveness of the deployed TM system. These indicators can also help organizations in a number of other ways. For example, KRIs can help track an organization’s risk appetite and also can help identify potential emerging risks (i.e., regulatory changes, industry standardization) and drive appropriate risk mitigation activities. KPIs can help organizations analyze historical data and allow for pattern recognition and forecasting – which can be utilized in the areas of alert management and capacity planning.

Figure 1. Definition of KRIs and KPIs in the TM process

<table>
<thead>
<tr>
<th>KRIs</th>
<th>Definition: Metrics used by organizations to provide an early signal of increasing risk exposures in various areas of the enterprise.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Examples: Alert handling; investigation and volume of alerts generated; introduction of new regulations and industry benchmarks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>KPIs</th>
<th>Definition: Metrics that provide a high-level overview of an organization’s performance and/or the performance of its operating units with a focus on historical performance.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Examples: Reports highlighting monthly, quarterly, and year-to-date number of alerts processed; trends in alert backlogs and submitted SARs.</td>
</tr>
</tbody>
</table>

KPIs and KRIs can and should be leveraged to uncover and address areas of inefficiencies in the end-to-end TM process. Below are examples of indicators pointing to an ineffective TM system or process:

<table>
<thead>
<tr>
<th>Indicators of Operational Issues</th>
<th>Indicators of TM System Ineffectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Substantial backlogs and late alert closures/SAR filings</td>
<td>• Certain transaction types never seem to generate alerts.</td>
</tr>
<tr>
<td>• Sudden spikes or significant decreases in alert volumes from one month to the next</td>
<td>• Many high-risk customers never seem to generate alerts.</td>
</tr>
<tr>
<td>• Frequently late SAR filings affecting the submission deadline</td>
<td>• Number of manual referrals exceeds referrals from system-generated alerts.</td>
</tr>
<tr>
<td>• High or low conversion rates (too many or too few) of alerts converted to SARs</td>
<td>• The system generates a high percentage of recurring alerts on the same customers, even though those customers were previously investigated and deemed not suspicious as activity is consistent with the nature of their business/account.</td>
</tr>
</tbody>
</table>
Measurements obtained from TM activities are key in helping different audiences within the organization track such indicators of performance, identify areas of inefficiencies and monitor risk appetite thresholds. The list below includes most, but not all, metrics that can be obtained from the TM system:

- Number of alerts generated (by scenario)
- Number of alerts by product line/service
- Number of alerts escalated to cases
- Percentage of alerts converted to investigations
- Number of alerts closed
- Number of cases identified manually
- Number of alerts escalated to cases by scenarios
- Number of alerts generated by high-risk jurisdictions
- Percentage of alerts generated by high-risk jurisdictions
- Alerts by line of business (where originated)
- Number of alerts/cases with request for information (RFIs)
- Number of alerts/cases with RFIs not addressed within a certain number of days
- Number of cases closed
- Number of cases not closed within 30, 60, 90 or 180 days

To get to these correct metrics, we recommend institutions take the following steps with regard to data, governance and reporting:

**Data Considerations**

- Review data sets to verify the accuracy, completeness and availability of appropriate data elements (parameters) feeding into reports.
- Review historical records associated with a repository/data source to determine if any filters are impacting the data quality. For example, for data sources that are not supported by good documentation, perform testing and root cause analysis to identify filters, transformation rules, etc.
- Establish data lineage to ensure that the appropriate data is being extracted for metric calculations and all data transformation rules are identified and assessed.
- Create a data mart to aggregate data from disparate systems and have one system of record for generating reports. Tightly integrate the TM and case management systems to leverage business intelligence developed at the investigation level.

**Metrics and Governance Considerations**

- Develop effective metrics using the correct parameters. Ask yourself if what is being measured is in fact what is required by the business to answer questions about risk exposure or performance.
- From a governance perspective, clearly define a process to help record the metrics being produced as part of the alert management process (e.g., false positive alerts, suspected SARs, actual SARs generated, alert volumes, etc.). Manage business user expectations and align/rationalize business requirements where possible through working sessions.
• Establish drivers for business requirements and determine if the same solution should be applied to meet similar sets of requirements.
• Centrally manage initiatives and review against enterprise strategies and goals to ensure alignment. This will minimize duplicated effort, identify opportunities for synergies between projects/initiatives and effectively leverage the right resources across the organization.
• Establish governance committees to review project progress and identify instances of deviations from initial proposals/objectives in order to reassess effectively the value derived.

**Reporting Considerations**

• Establish a user interface that references the data mart from which users (e.g., the business) can generate pre-established reports.
• Allow users to create ad hoc reports from the user interface. Ad hoc reports call to a refreshed data set at the moment the user creates the report. This enables users to get reports with the most up-to-date data, as well as view only the data they want to view, saving users’ time.

Combining the use of metrics, data analytics, AML technology and suspicious activity monitoring can help managers and stakeholders at financial institutions to:
• Provide information on risks affecting the organization
• Use better information in real time to ensure compliance with current local regulations
• Become aware of whether current business practices meet regulatory requirements and are aligned with organizational risk strategy
• View cross-business and jurisdictional transactions for easy identification of trends and exceptions
• Determine if existing TM systems and processes require enhancement using operational and system indicators
• Re-estimate targets for each metric and assess the operational impact of the alerts on time, cost and resources
• Provide data for applying techniques such as scenario analysis, black-box testing, data quality reviews, etc.
• Identify the root cause(s) of an ineffective program
• Develop targeted solutions based on root cause analysis completed
• Refine the TM approach, technology, methodology and templates based on key observations, trends and identification of high-risk indicators
Internal Audit’s Expanded Role in Assessing AML Technology

**Issue**

Transaction monitoring (TM) and sanctions screening systems are invaluable tools in the never-ending effort by financial institutions to detect potential money laundering activity effectively and efficiently. Many institutions invest significantly in implementing anti-money-laundering (AML) technology but then fail to maximize its potential and capabilities, often leaving gaps in their compliance efforts.

The notion that AML technology can be installed with minimal customization and left to operate virtually autonomously is naïve – especially in an era of intensifying regulatory scrutiny. Without appropriate control procedures, significant operational errors can occur, including an excessive amount of false positives and false negatives (instances of money laundering that go undetected). The regulatory emphasis on detecting such instances and the increasing complexity and integration of AML technologies require internal audit (IA) to transform the way it assesses AML systems to help protect the institution.

**Challenges and Opportunities**

In our experience, financial institutions encounter several challenges in establishing a governance framework with proper controls to ensure that transaction monitoring systems are operating properly and evolving as necessary. These challenges include:

- **Adapting to stricter regulatory standards.** With the evolution of transaction monitoring and sanctions screening technologies, the required transparency of the processes and controls that support the technologies has increased. Specific areas of focus include assurance of data integrity, fine-tuning of monitoring scenarios, validation of system effectiveness, appropriate backup and recovery and inclusion of privacy considerations.

- **Improving IA’s knowledge of AML technologies.** The rapid enhancement and sophistication of AML technologies are creating a knowledge gap for some institutions’ IA staff. In today’s business environment, internal auditors need to be intimately familiar with the way AML systems work, including the testing, fine-tuning and validating of these systems.

- **Integration of skills.** The use of transaction monitoring and sanctions screening systems is not just an IT issue. IA needs to have an integrated team of people with compliance, business and technology skills to assess AML technology effectively.

- **Understanding IA’s role in assessing AML technology systems.** Responsibilities for ensuring effective deployment and maintenance of AML technology is shared among multiple parties, and the roles and responsibilities of each party must be clearly delineated.
By addressing the challenges above, financial institutions and their IA functions will be better positioned to assess and improve their AML technology and the supporting processes and increase the effectiveness and sustainability of their TM programs.

**Our Point of View**

Even the most sophisticated transaction monitoring and sanctions screening systems are of minimal value unless they operate in an environment with appropriate control procedures. In light of heightening regulatory expectations, financial institutions should re-evaluate and bolster IA’s role in ensuring a proper governance framework and oversight for effective, sustainable and repeatable processes and controls.

The following table outlines the various AML technology responsibilities of the three “lines of defense” inside an institution. While many responsibilities cut across the lines of defense, the table highlights IA’s potential responsibilities related to assessing AML technology.

<table>
<thead>
<tr>
<th>Line of Defense</th>
<th>AML Technology Responsibilities</th>
</tr>
</thead>
</table>
| First line of defense (e.g., operations, IT) | • Utilize various AML technologies, including but not limited to transaction monitoring (TM), Know Your Customer (KYC) and sanctions screening, to prevent certain transactions from occurring as well as to gather information to be utilized by the compliance organization.  
• Provide ongoing maintenance and production support of the systems and data processes.                                                                                                                                                                                                                      |
| Second line of defense (e.g., compliance, risk management, IT) | • Utilize the output of various AML systems (e.g., TM, KYC, sanctions screening) to identify and report suspicious activity.  
• Periodically tune thresholds to ensure appropriate coverage and possible optimization of values.  
• Perform a model validation of AML technology systems that addresses the regulators’ model validation guidance (OCC Bulletin 2011-12 and FRB SR 11-7).  
• Ensure appropriate technology controls in the areas of security, change management, on-going data integrity and backup and recovery.                                                                                                                                 |
| Third line of defense (e.g., IA) | • Review the validation and tuning processes to ensure that an appropriate methodology and approach are executed in accordance with requirements.  
• Review IT processes (e.g., ongoing data integrity and reconciliation checks, change management, security, backup and recovery) and configurable controls (e.g., system overrides, workflow).                                                                                                                                                      |

With a clear understanding of its role and responsibilities as a third line of defense, IA is positioned to design and perform a comprehensive AML technology audit. Key audit areas to ensure adequate coverage are: establishing procedures for data integrity; security; change management; and back-up and recovery.

- **Data integrity.** Financial institutions frequently overlook the importance of the completeness and accuracy of data sets used in transaction monitoring and sanctions screening systems. They also may underestimate the effort needed to identify and integrate data from across the institution, which requires the collection of customer, account and transaction information. In both cases, incomplete or inaccurate data will undermine a transaction monitoring system’s ability to operate optimally. IA needs to verify that procedures are in place and operating on an ongoing basis to identify and resolve data quality and data-load issues.

- **Security.** Security and privacy requirements should be determined for the output (e.g., alerts) of the AML technology. Privacy requirements and financial institution policy may drive access requirements for alerts and customer information based on geographic region or type of activity (e.g., private banking, alerts on employees). IA needs to ensure that alert and investigation workflows are established with appropriate segregation of duties in place to prevent users from approving their own work.
addition, security controls should be implemented across the technology layers (e.g., operating system, database management system) to ensure that access to critical data elements (e.g., customer, account, transaction) is appropriately restricted.

- **Change management.** A comprehensive change management process needs to be in place to ensure that any type of change to the system in the production environment has been through a testing and approval cycle. For example, changes to the threshold values of the deployed scenarios or alteration to the workflow process should follow the change management process.

- **Backup and recovery.** IA needs to ensure there is a systematic backup and recovery process in place that aligns with the financial institution’s recovery objectives.

If an institution is implementing new AML technology, IA’s role takes on additional dimensions. In addition to the areas mentioned above, responsibilities broaden to oversee testing strategies and organizational change management.

- **Testing strategies.** During implementation, IA needs to play a critical role to ensure that the product team executes the required tasks. IA’s mission in this capacity centers on preparing and asking the right questions, for example:
  - Is testing comprehensive enough to verify that the system is operating as intended?
  - What testing is being done to make sure that data is accurate?
  - Has the institution completed an adequate inventory of the customer and transaction systems that will feed the newly implemented AML technology?

Testing includes assessing potential limitations of the system and evaluating the system’s operation over a range of input values. Specifically, this step should include user acceptance testing – ensuring that users, in a controlled environment, understand how the system functions and can operate it to achieve desired outcomes. So-called “negative testing,” using artificial sample data, should be included to detect transactions that should have resulted in alerts but failed to generate them.

- **Organizational change management.** The impact new AML technology has on an institution depends on the type and complexity of the AML technology, as well as the scope of the implementation (e.g., geographic, business unit). IA should assess more than just the AML technology and ensure all areas impacted by the AML technology are also considered. The following are some questions that IA should consider as part of its assessment:
  - How will the new AML technology and related procedures impact customers (e.g., on-boarding)?
  - Will current transaction and customer data need to be improved to ensure an effective use of the AML technology?
  - How will compliance processes (e.g., closing of alerts, investigations) change to incorporate different information provided by AML technology?
  - What management reports will need to be created or modified to determine and communicate effectiveness of the AML technology?
Examples of Protiviti’s Work With AML Transaction Monitoring Systems

Model Validation of Multiple Sanctions Screening Systems

A top-25 U.S. bank engaged Protiviti to perform a model validation of the quantitative aspects of its sanctions screening models. The validation scope consisted of eight different list screening systems used across multiple business segments within the bank. We developed a scenario-based methodology, which utilized fuzzy matching techniques, good and bad samples and various combinations of regulatory watch lists to test the performance of each system on a stand-alone basis and relative to other systems. Fuzzy matching techniques were used to mask names and other transaction details to assess the ability of each system to detect small variations of regulatory watch list entries.

Our deliverables consisted of a report noting gaps and findings, along with recommendations for tuning the current score thresholds within the bank’s sanctions screening systems. In the report, we identified which transaction components are most predictive of true positives on a system-by-system basis (by matching multiple fields, such as name, address and date of birth, rather than a single field). In addition, we uncovered potential cost savings for the bank by identifying which systems had very similar scoring mechanisms and could be consolidated to reduce screening efforts. Our report included the detailed testing procedures, validation methodology, and analyses of scoring thresholds within each system in terms of true positive and false positive rates. Leveraging our findings and recommendations, the bank was able to address critical gaps in its sanctions compliance and improve the efficiency of its program.

Reducing False Positives Through a Qualitative Approach

A large bank engaged Protiviti to assist with threshold tuning of its existing scenarios. We developed a systematic threshold-setting and tuning methodology that not only took into account the quantitative aspects of these scenarios, but also the qualitative aspect of alert reviews in order to determine the final threshold values that the client should deploy in production.

Our deliverables consisted of a documented methodology and approach to assess periodically the appropriateness of scenarios and thresholds both from a quantitative and qualitative perspective, software scripts that the bank could leverage on an ongoing basis to perform threshold setting and tuning, sampled alerts and investigation lite review results. By leveraging this qualitative approach, the bank was able to reduce potential false positives, improving investigator efficiency.
Using Functional Criteria to Perform AML System Selection

A multi-bank holding company requested our assistance with assessing multiple systems to identify the optimal sanctions screening software to support its AML and OFAC program. Protiviti developed matrices with weighted vendor, performance, functional and technical criteria to facilitate the comparative analysis of each type of software. The evaluation criteria were based on previous experience with various types of systems, user and system manuals, research, and discussions with the bank’s power users and management. At the end of the engagement, we provided analysis ratings of the different software solutions based on the identified functional and technical criteria to summarize the key strengths and weaknesses of each system.

Using Key Metrics to Enhance Management Information Reporting

A large global bank sought our assistance to enhance AML management information reports in order to identify improvement opportunities in its end-to-end transaction monitoring systems and supporting processes. Our integrated team of AML and Business Intelligence experts performed a data quality review, identified key metrics, and developed dashboards which successfully helped our client in enhancing its MI reporting process. Our work helped the client achieve the following:

- **Enhanced usefulness and reliability of data.** We generated reports on data quality and completeness, which allowed the institution to identify areas of increased risk (where data was incomplete) and re-prioritize remediation efforts to fix the data issues and increase its monitoring coverage.
- **Operating effectiveness and increasingly mature TM processes.** We created customized reports that provided middle management with real-time information on alert clearing productivity. These reports prompted the institution to find a different method for managing the alerts, which resulted in reduced headcount and costs.
- **Management information governance framework.** The governance framework we implemented allowed the institution to set in place procedures to review and update MI reports on an ongoing basis to ensure accuracy and timeliness, creating a sustainable reporting environment.
- **Improved reporting to regulators.** The accurate and timely MI reports on the end-to-end TM process enabled senior management to substantiate its discussions with regulators by using the MI reports to support its messages.

Identifying Monitoring Gaps as a Result of TM and Sanctions Screening System Audit

A global financial institution sought our assistance performing an audit of its TM and sanctions screening applications. The audit scope included the areas of data integrity, change management, security and functionality. We worked together with the business and technology personnel from the bank to obtain a clear understanding of existing processes and controls, and collected sample data sets to perform the audit. We were able to identify gaps in the sanctions screening system, which were caused by a lack of appropriate change management and security controls. As a result of our review, the bank took steps to close the gaps in the monitoring scenarios and adjust the thresholds, reducing the number of false positives.
About Protiviti

Protiviti ([www.protiviti.com](http://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 40 percent of FORTUNE 1000® and FORTUNE Global 500® companies. Protiviti and its independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. The firm also works 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 (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

How Protiviti Can Help

Whether your financial institution is implementing an AML transaction monitoring system for the first time, changing vendors and systems, or performing periodic review and maintenance of current systems, Protiviti has the experience and resources to help. Below is a short summary of how we can assist your financial institution in each of the five stages discussed in this white paper.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning</td>
<td>• Review to ensure program is risk based</td>
</tr>
<tr>
<td>Implementation</td>
<td>• Review data feeds and data integrity</td>
</tr>
<tr>
<td></td>
<td>• Assist in the development of rules and parameters</td>
</tr>
<tr>
<td>Pilot testing</td>
<td>• Review to ensure policies and procedures are appropriate</td>
</tr>
<tr>
<td></td>
<td>• Review to ensure management/users have adequate knowledge</td>
</tr>
<tr>
<td></td>
<td>• Provide training to end users and refresher training for management</td>
</tr>
<tr>
<td></td>
<td>• Perform pilot testing to understand whether initial parameters for rules are effective/efficient</td>
</tr>
<tr>
<td>Alert review and trend analysis</td>
<td>• Evaluate system configurations using worst-case scenarios</td>
</tr>
<tr>
<td></td>
<td>• Evaluate system for adequate coverage of financial institution’s profile</td>
</tr>
<tr>
<td></td>
<td>• Provide support to clear accumulated backlogs</td>
</tr>
<tr>
<td>Maintenance of the monitoring program</td>
<td>• Provide recommendations for improving system effectiveness and efficiency based on changes at the financial institution</td>
</tr>
<tr>
<td></td>
<td>• Assist in the validation of risk assessment based on monitoring system trends</td>
</tr>
<tr>
<td></td>
<td>• Perform periodic reviews of the monitoring system</td>
</tr>
</tbody>
</table>

For additional information about the issues reviewed here or Protiviti’s services, please contact:

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

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

John Atkinson  
Director  
+1.404.926.4347  
john.atkinson@protiviti.com

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

Luis Canelon  
Associate Director  
+44.20.7024.7509  
luis.canelon@protiviti.co.uk

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

For additional information about the issues reviewed here or Protiviti’s services, please contact:
### THE AMERICAS

**UNITED STATES**
- Alexandria
- Atlanta
- Baltimore
- Boston
- Charlotte
- Chicago
- Cincinnati
- Cleveland
- Dallas
- Denver
- Fort Lauderdale
- Houston

**ARGENTINA***
- Buenos Aires

**BRAZIL***
- Rio de Janeiro
- São Paulo

**CANADA**
- Kitchener-Waterloo
- Toronto

**ASIA-PACIFIC**

**AUSTRALIA**
- Brisbane
- Canberra
- Melbourne
- Perth
- Sydney

**CHINA**
- Beijing
- Hong Kong
- Shanghai
- Shenzhen

**INDIA***
- Bangalore
- Mumbai
- New Delhi

**INDONESIA**
- Jakarta

**JAPAN**
- Osaka
- Tokyo

**SOUTH KOREA**
- Seoul

**PHILIPPINES**
- Manila

**THAILAND**
- Bangkok

**THAILAND**
- Pattaya

**TAIWAN**
- Taipei

**VIETNAM**
- Hanoi
- Saigon


### EUROPE/MIDDLE EAST/AFRICA

**FRANCE**
- Paris

**GERMANY**
- Frankfurt
- Munich

**ITALY**
- Milan
- Rome
- Turin

**THE NETHERLANDS**
- Amsterdam

**BAHRAIN***
- Manama

**KUWAIT***
- Kuwait City

**OMAN***
- Muscat

**SOUTH AFRICA***
- Johannesburg

**THE AMERICAS**

**UNIFIED STATES**
- Alexandria
- Atlanta
- Baltimore
- Boston
- Charlotte
- Chicago
- Cincinnati
- Cleveland
- Dallas
- Denver
- Fort Lauderdale
- Houston

**ARGENTINA***
- Buenos Aires

**BRAZIL***
- Rio de Janeiro
- São Paulo

**CANADA**
- Kitchener-Waterloo
- Toronto

**ASIA-PACIFIC**

**AUSTRALIA**
- Brisbane
- Canberra
- Melbourne
- Perth
- Sydney

**CHINA**
- Beijing
- Hong Kong
- Shanghai
- Shenzhen

**INDIA***
- Bangalore
- Mumbai
- New Delhi

**INDONESIA**
- Jakarta

**JAPAN**
- Osaka
- Tokyo

**SOUTH KOREA**
- Seoul

**THAILAND**
- Pattaya

**TAIWAN**
- Taipei

**VIETNAM**
- Hanoi
- Saigon

---

* Protiviti Member Firm
** Protiviti Alliance Member