ACAMS Advanced Certification White Paper: Independent Audit and Insurance AML Transaction Monitoring
Vicki Landon, CAMS, FLMI, CFCS

The Bank Secrecy Act (BSA) requires that insurance companies identify and report suspicious activities, which is the ultimate goal of transaction monitoring. Companies are free to choose how they monitor transactions – via manual processes, exception reports, and/or transaction monitoring systems (TMSs) – as appropriate for their size and risk profile, as long as the method(s) effectively identify suspicious activities and support timely reporting.

To ensure effectiveness, regulations require that life and annuity insurers test their transaction monitoring periodically as part of the required independent testing or audit. The Federal Financial Institutions Examination Council (FFIEC) BSA/Anti-Money Laundering (AML) Examination Manual states that “Independent testing should, at a minimum, include...a review of the effectiveness of the suspicious activity monitoring systems (manual, automated, or a combination) used for BSA/AML compliance.”¹ It instructs examiners to verify the adequacy of the independent audit:

“Determine whether the audit’s review of suspicious activity monitoring systems includes an evaluation of the system’s ability to identify unusual activity. Ensure through a validation of the auditor’s reports and work papers that the bank’s independent testing:

- Reviews policies, procedures, and processes for suspicious activity monitoring.
- Evaluates the system’s methodology for establishing and applying expected activity or filtering criteria.
- Evaluates the system’s ability to generate monitoring reports.
- Determines whether the system filtering criteria are reasonable and include, at a minimum, cash, monetary instruments, funds transfers, and other higher-risk products, services, customers, or geographies, as appropriate.”²

The BSA/AML Examination Manual for Money Services Businesses, which the IRS has been using as a primary guideline for examining insurance companies until the final version of the BSA/AML Insurance Examination Manual is made available, stipulates that “…the review should include testing of internal controls and transactional systems and procedures to identify problems and weaknesses and, if necessary, recommend to management appropriate corrective actions.”³ It guides the IRS examiner in testing the TMS to determine the adequacy of its controls.

---

² Ibid. pp. 40-41
Besides these publications, attending industry events and networking, how can insurance companies know what regulators expect regarding the independent audit of their transaction monitoring systems?

Regulators set expectations via enforcement actions concerning financial institutions whose independent testing failed to assess the effectiveness of their TMSs and demanded corrective action (see Enforcement Actions, below). Regulators expect that financial institutions using a TMS validate the integrity and accuracy of the data and systems. They also expect that scenarios, filtering criteria and thresholds reflect the risks exposed in the AML Risk Assessment. As the July 17, 2013 edition of ACAMS moneylaundering.com CTF Wrap-up stated, “Bad audits remain a common thread of costly regulatory penalties.”

However, life insurance and annuity companies face significant challenges in conducting such tests on automated TMSs. This white paper is intended to explore those challenges and regulators’ expectations, and to suggest guidelines for scoping and for testing the effectiveness and efficacy of insurance AML exception reports and TMSs.

**Types of Transaction Monitoring Systems in Insurance**
The TMSs available today range from manual processes and simple exception reports to sophisticated, multidimensional, pattern-based, statistical sampling, and neural-network systems supporting an array of industry typologies.\(^5\) For the purposes of this paper, TMSs include automated systems that evaluate transactions through the use of some or all of the following:

- Scenarios (business cases representing typologies of money laundering or terrorist financing, often reflecting patterns of activity over time)
- Filtering criteria (selection criteria which determine whether a transaction is tested for a given scenario)
- Thresholds (the level represented in data, including dates, counts, amounts, etc., at which a transaction generates an alert, e.g. surrender penalty amount or number of months after issue)
- Risk-ranking of customers

These TMSs generally are capable of evaluating client-level activity across multiple contracts and providing customer profiles and customer risk assessments.

**Enforcement Actions and Independent Testing of TMSs**
Regulators have expressed their expectations in recent enforcement actions, which can help guide insurers in determining the extent to which they are expected to test TMSs regularly and during

---

4 ACAMS moneylaundering.com CTR CFT Wrap-up Covering July 10-16, Kieran Beer, July 17, 2013
independent audits. For example the Pamrapo assessment (6/2010) called out the lack of BSA training and experience of the Internal Audit Staff that failed to detect defects in the TMS such as coding errors that for years enabled individuals to structure transactions without risk of detection.\(^6\)

The most egregious and systemic AML failures have been blamed in part on failure to adequately test the TMS, such as the following cases, which include direct criticisms of the independent audit processes that enabled each of these financial institutions to continue with inadequate AML programs for year after year.

- The Citibank consent order in April, 2012, cited an inadequate independent audit function that failed to identify systemic deficiencies, due in part to weaknesses in the scope of the validation and optimization process applied to the automated TMS\(^7\).

In one of the most prescriptive and exacting sets of instructions regarding a company’s TMS, the Comptroller ORDERED (capitalized in the original order) the bank to retain an independent consultant within 30 days to evaluate the processes for identification of suspicious activity, including an extensive assessment of the TMS. Management was required to ensure (emphasis added) an extensive list of TMS functions including:

- An electronic due diligence database readily accessible to the relationship manager or others;
- Data integrity feeding the TMS;
- Sufficient tailoring of the system to the bank’s risk profile and operations;
- Full utilization of the system’s functionality;
- Appropriateness and effectiveness of scenarios and rules in identifying unreasonable or abnormal client activity;
- Sufficient management information and metrics to manage and adjust the system;
- Statistically valid processes to validate and optimize TMS settings and thresholds and measure the effectiveness of the automated system;
- Alert scoring methodology to prioritize workflows and facilitate management of the system and the ongoing validation / optimization of system settings;
- Adequacy of staffing to investigate and clear alerts;
- Quality and completeness of information available to staff monitoring alerts and conducting investigations, including information from multiple lines of business a customer transacts;
- Standards and documentation for dispositioning alerts;
- EDD for customers with a high volume of alerts, and for higher-risk clients and/or products or services;
- Sufficient quality control processes to ensure the TMS, alert management process; and

---

\(^6\) Pamrapo Savings Bank, S.L.A. Assessment of Civil Money Penalty, 6/2010, pp. 2-4

\(^7\) Citibank Consent Order, 4/5/2012, p. 3
- SAR decision making and filing are working effectively and according to internal standards.\(^8\)

- Ocean Bank’s Assessment of Civil Money Penalty of August 2011 found the bank’s independent testing ineffective and failing to ensure compliance with the BSA, particularly in that it did not adequately test the TMS and reporting systems. It implemented an automated TMS, but only loaded 15 percent of its accounts, which nevertheless created a backlog of more than 100,000 alerts within three years. Many high-risk transactions were not monitored at all. Even relatively obvious individual transactions – such as large round wire transactions for tens of thousands of dollars, inconsistent with company profiles and geographies and lacking business purpose – were not flagged as suspicious. Ocean Bank failed to document or explain account filtering criteria or thresholds, or how these were appropriate for the bank’s risk. The bank failed to periodically review and update the filtering criteria and thresholds, thus “rendering them ineffective.” The TMS’s programming, methodology, and effectiveness were not independently validated until six years after implementation, so it was impossible to verify if the models were detecting potentially suspicious activity. The Federal Deposit Insurance Corporation (FDIC) and Financial Crimes Enforcement Network (FinCEN) determined that the bank’s TMS “continued to be ineffective in identifying suspicious activity.” \(^9\)

- But Wachovia’s Assessment of Civil Money Penalty in March 2010 earned the bank perhaps the most extensive criticism for its independent audits’ failure to detect systemic deficiencies in the TMSs, which were judged to be inadequate to support the volume, scope, and nature of the bank’s business. The systems were not designed to readily identify suspicious elements, red flags or suspicious activity associated with individual transactions. Moreover, the monitoring system’s programming, methodology, and effectiveness were not independently validated to ensure that the models were detecting potentially suspicious activity. Worse yet, the independent audit failed to discover that the number of alerts generated was capped to accommodate the number of available compliance personnel. The TMS was “routinely tuned so that the number of alerts generated with respect to international correspondent banks remained constant at around 300 each month.”\(^10\) In fact, the bank limited the flagging and review of transactions for suspicious activities based on the inadequate number of staff available to review alerts. Like Ocean Bank, Wachovia’s BSA management failed to explain filtering criteria and thresholds. Wachovia likewise failed to specify how these criteria and thresholds were appropriate for the bank’s risks or update them as risks changed. Most significantly, the independent audit failed for years to detect these deficiencies.

In these and other enforcement actions, the financial institution’s internal audit function did not adequately evaluate and test the suspicious activity monitoring systems. These lessons show that testing the TMS is a critical step in ensuring that compliance problems are surfaced and corrected before

---

8 Citibank Consent Order, pp. 11-15
9 Ocean Bank Assessment of Civil Money Penalty, 8/22/2011, pp. 4-5
10 Wachovia Bank Assessment of Civil Money Penalty, 3/12/2010, p. 4
they are compounded, year after year, resulting in significant flaws in AML controls. The lesson for insurers is clear: it is necessary to establish a reasonable scope and frequency for independent audit’s testing of their TMSs and must ensure that internal auditors follow through.

**Insurers Face Unique Challenges**

Insurers face significant challenges in divining and meeting these expectations. While the banking industry has gained sophistication in its AML risk models, insurance has lagged behind for several reasons.

*Mixed Regulatory Environment*

Life and annuity companies exist in a mixed regulatory environment. While each bank or broker-dealer has its assigned regulator, insurance is regulated by each state and, for specific functions, also by federal regulators. When AML regulations were enforced for insurers in 2006, FinCEN appointed the IRS as its agent to perform BSA/AML examinations.

After six years of IRS examinations of insurers, FinCEN initiated discussions with the National Association of Insurance Commissioners (NAIC) to discuss having the states’ Departments of Insurance participate in the process. Several factors led to these discussions, according to former Director of FinCEN James Freis, who pointed out in his address to the American Council of Life Insurers on July 17, 2013, that business activities and compliance issues are closely linked and that “it is an efficient and effective approach to help FinCEN to have the insights of the licensing authorities and prudential regulators that know the industry best.”  

FinCEN and the NAIC reached an agreement early in 2012 to incorporate the initial BSA/AML examination (or “expanded inquiry”) within the regulatory examinations performed by the Department of Insurance of each company’s domiciliary state. FinCEN has been working with states’ insurance commissioners to build on that agreement with two types of Memoranda of Understanding (MOU), regarding the sharing of information in the context of regulatory exams, and concerning the sharing of information with respect to investigations of possible criminal activity.

Some states have already begun including BSA/AML inquiries in their regulatory examinations. These are guided by the NAIC Financial Conditions Examiners Handbook, which points out that state regulators are not expected to conduct a full-scope AML examination (which is the provenance of the primary federal regulator), but explains the procedures that should be included by the state examiners. According to Freis, the expectation is that, if the state finds issues with a company’s AML program, it refers the situation to FinCEN, which would work with together with the state in terms of remediation. If egregious cases are found, the companies will be penalized.

---

11 Remarks by James Freis, Counsel, Cleary, Gottlieb, Steen & Hamilton, and former FinCEN Director, in his session Emergence & Convergence of Regulatory Compliance Expectations, American Council of Life Insurers (ACLI) Compliance & Legal Section Annual Meeting, Orlando, FL, July 17, 2013, and in email to author 7/29/2013

12 NAIC Financial Condition Examination Handbook 2012, Section 1.c., pp. 98-101

13 James Freis, ibid.
And yet no enforcement actions have been issued for the insurance industry. Insurers seek guidance in enforcement actions written for other industries, interpreting and applying findings as is reasonable.

The result of this compliance milieu is that regulatory expectations for life and annuity companies are not black and white, but are evolving.

**Legacy Systems**

While banks or broker-dealers might have “siloed” systems that are as old as 10-20 years, insurers often have a few or dozens of legacy administrative systems that have been around for 50 years, because of the length of insurance contracts, mergers and acquisitions, and the expense of system conversion. Most of these systems organize data at the contract level rather than the client level. Data in these systems is frequently missing or unreliable, and the processes to map the old data to the new TMS and then extract, transform and load are challenging and expensive. After the data is loaded into the TMS, clients are usually replicated with each policy or contract (i.e., one customer with two policies appears as two unrelated customers in the system) and often are associated with outdated demographic data. These factors add challenges for data analysts in developing thresholds based on sound logic and statistics.

**Industry Specific Scenarios**

When an insurer implements a TMS that is oriented towards depository institutions, the insurer must add insurance-specific scenarios, such as patterns of loans and loan repayments, numbers of “free looks” per client, premiums paid in advance, paid up additions with surrenders, and behavior of agents. The Financial Action Task Force (FATF) has provided a platform of common insurance AML scenarios, along with guidance in determining level of customer risk, in its *Risk-Based Approach: Guidance for the Life Insurance Sector.*

Creating and tuning thresholds of typologies is a daunting task. Moreover, there is not much published record of trends in insurance money laundering typologies. Each company has to figure out the money laundering typologies that pose a risk in each business unit, the red flags to detect them, and the thresholds that will generate a solid ratio of alerts that lead to Suspicious Activity Reports (SARs).

Finally, it is challenging for a company to justify the expense of a TMS, when the government has not yet fined an insurance company for AML failures. For companies that take the less expensive path of writing exception reports, it is challenging to justify the reports’ usefulness when it is very rare to find a SAR filed by an insurer based on information in an exception report.

---

Testing the TMS

Despite these challenges, an independent AML audit is expected to test a company’s TMS. This testing of the transaction monitoring environment is risk-based, like other aspects of the independent audit. The methods described below enable reasonable testing of the TMS without requiring the auditor to conduct a full-scale system test and optimization – both lengthy and expensive operations. Rather, these steps are designed to be realistically within the budget and timeframe of an independent audit while enabling the auditor to make a reasonable determination as to the ability of the TMS to identify and report suspicious activity.

The testing includes four phases:

1. **Data validation**: Ensure that data has been correctly mapped, transformed and loaded into the exception reporting or transaction monitoring system.
2. **Alerts triggered as intended**: Verify that the TMS is triggering alerts correctly when thresholds are hit.
3. **Case management and reporting**: Ensure that alerts are being properly investigated, documented and dispositioned, and SARs and Forms 8300 are being created, filed and maintained in a timely manner.
4. **Appropriate tuning**: Verify that there is adequate rationale for the parameters, thresholds, filters and rule settings.

These phases and sample activities included in them are explained below, along with suggestions for actions the independent auditor can take if necessary. While these steps are traditionally included in responsible systems management, the requirement for each recommendation is also put into the context of the relevant enforcement actions mentioned above.

1. **Data Validation**

The foundation of automated transaction monitoring is the transaction data. If the data lacks integrity – that is, if it is inaccurate, incomplete or incorrectly understood and mapped, the TMS is inherently unreliable. Although there is no way to guarantee 100 percent accuracy over time, there are ways to ensure data is substantially correct and being loaded successfully into the TMS. These steps can happen independently according to the risk of a subset of data and transactions and the availability of resources.

- Verify that appropriate data and transactions are accurately mapped. The independent auditor can reasonably verify this by reviewing documentation on the mapping of data from the original implementation and after any changes were made to the source systems or the TMS. The auditor should pay particular attention to the data and transactions that present the highest risk, such as loans, partial withdrawals, free looks, and surrenders.
The auditor should also ask about processes used to ensure all relevant data sources were located. For example, insurance companies often have tangential reports or databases to supplement old, low-function administrative and payout systems. There should be some documentation that the implementation team searched for any such extra data stores.

A complete data validation exercise is time-consuming and expensive. If the auditor has reservations about data integrity and the mapping and control processes covering data, the auditor should consider recommending that full data validation be undertaken.

- Verify the processes to ensure that data and transactions are successfully loaded. The auditor should question the processes by which IT is confident that all appropriate data from all source systems was successfully loaded each day. There are numerous methods to accomplish this. The most basic includes automated processes to balance data files extracted from each source system to the data loaded into the TMS, notifying operators of any data that did not load because of incorrect codes or malformations. Additional verification should be conducted, for example that all covered policies have been loaded and that all financial transactions of those policies are loaded, either by counts or sample tests.

If there is no balancing process, the auditor should recommend developing one. If there is not enough confidence in the integrity of the data, the auditor should recommend a test of the data mapping and the extract/transform/load process.

- Verify that there is a process to update and test the extract/transform/load programs whenever a change is made to the source systems or the TMS. If there is not a documented process in place, the auditor should recommend the IT department develop it.

These data verification steps are crucial to the integrity of any TMS. The critical nature of verifying the data’s completeness and accuracy is underscored by three of the enforcement actions mentioned above:

- The Citibank Consent Order pointed out the effect of the independent audit failing to find the data integrity issues in the TMS.
- The Pamrapo Savings Bank Assessment of Money Penalty illustrates the danger of failing to properly map data from the source system to the TMS, as coding deficiencies did not allow the system to detect the structuring of transactions.
- The Ocean Bank civil money penalty found that significant amounts of data (85 percent of accounts) were not successfully loaded into the TMS, and that the integrity of the data was not independently validated for a period of six years after being put into production. At a minimum, this kind of oversight means the
TMS cannot evaluate the customer’s activity across the enterprise, much less screen activities in the 85 percent of accounts not loaded.

2. Alerts and Reports Triggering as Intended
The point of this step is to verify that the TMS is indeed generating alerts as intended. While a basic step, this testing is generally overlooked.

- Verify that the business regularly tests that alerts are being triggered as intended. This includes testing that the appropriate transactions for all lines of business are generating alerts when the triggering criteria are met. It also includes negative testing – that is, verifying that alerts are not triggered by amounts that are just under or just over the threshold amount.

This step requires the use of test data, generally structured as a regression test that can be run periodically and particularly after changes to any source systems, the TMS, or the IT environment. If there has been no testing that alerts trigger correctly, the auditor should recommend conducting such tests through regression testing or other means.

This is the type of effectiveness testing that each of the institutions listed above failed to conduct.

3. Case Management and Reporting
Because timely, accurate reporting of suspicious activity is the goal of the BSA and USA PATRIOT Act, it is critical to track and time the handling of potentially suspicious alerts. Case management entails tracking each alert, logging all investigative actions and decisions, managing supporting documentation, documenting the decision to file or not file a SAR, and retaining a copy or electronic version of the filed report. It should support combining multiple related alerts or reports.

- Verify that alerts are being handled in a timely fashion, based on alert priority (if available in the TMS). This can be achieved by reviewing reports showing alerts generated, viewed, and dispositioned. If there are no such reports, the auditor should request the process by which the AML Compliance Officer (AMLCO) oversees and manages alert assignment. The absence of such a report or process indicates a serious weakness in the system controls and must be included in the audit report findings.

- Verify that alerts are being properly investigated and that the dispositioning is timely and well-documented. Jerry Danielson, AVP, Compliance Audit Director, Lincoln Financial Group, recommends this be achieved by sampling a number of alerts that were closed without action, that were escalated before being closed, that resulted in a Form 8300, and that resulted in a SAR. The auditor should review the
documentation supporting the decision, the timeliness of the disposition, and the appropriateness of the decision.¹⁵

- Verify that records are being appropriately maintained for a minimum of five years or the timeframe specified in the company’s AML program. This can be achieved by reviewing the records retention policies matched with TMS documentation, and by reviewing a sample of the SARs and Forms 8300 produced.

Many of the cited enforcement actions failed in this step, but two stand out: Citibank was cited for failing to have adequate staffing to deal with alerts in a timely fashion. Wachovia on the other hand reduced the number of alerts produced to meet the ability of the staff to deal with them. And the independent audits failed for years to find these deficiencies.

4. **Appropriate setting of thresholds, filtering criteria and parameters**

The best TMS is incapable of identifying suspicious activities if the AMLCO has not ensured that four processes occur: that the AML Risk Assessment accurately rate the risk associated with the company’s distribution channels, products, markets, services, operations and geographies; that appropriate AML staff learn the significance and use of each threshold and filter; that the AML team has access to meaningful statistics on each business unit’s business and agents; and the statistics and risk ratings inform the setting of thresholds, filtering criteria and parameters. Together, these might be called the variables of the TMS.

The tuning or optimization of the system is a time-consuming process that requires intimate knowledge of the system and the business. It would be difficult to include this time and expense in the audit’s scope. Fortunately there are steps the auditor can take to come to a reasonable conclusion as to the appropriateness of the thresholds, filters and parameters.

- Verify that the AML program includes documentation on the processes used to select and test the settings of variables. “Developing and maintaining proper documentation of any and all changes made to thresholds, including final tuning adjustments, are imperative to evidence the rationale and execution of the defined methodology and to provide a foundation for future tuning,” according to Luis Canelon, Carl Hatfield, and Chetan Shah of Protiviti.¹⁶

  - Verify that the setting of each variable is supported by statistics and/or other strong business rationale. For example, to determine how to set the minimum

---

¹⁶ Luis Canelon, Carl Hatfield, and Chetan Shah, Anti-money laundering transaction monitoring system implementation considerations, *Acams Today*, June-August 2013
threshold above which a CWA (Cash with Application) payment will require enhanced due diligence, it would be helpful to understand mean and median of CWA amounts. It would be very useful to have standard deviations for transactions, to establish outliers.

A useful way to verify this is to ask to see the scenarios that the AML staff hopes to catch, annotated with numbers from the risk assessment and statistical analysis. This would indicate that the AML staff used the Risk Assessment to determine the scenarios which present significant risk, and then rely on statistical analysis to determine the optimal risk-based settings for the associated variables.

- Verify that there is a governance process, including approvals, for changing any variable setting. Verify that there is documentation requesting any change to variable settings.

- Review the processes to determine the frequency with which variable settings are reviewed, and judge the adequacy of review timing based on the overall risk profile, changes to the product suites, changes to the business model, and the pace of regulatory changes.

- Review processes used by the AML staff to determine the effectiveness of the variable settings. Processes could include for example test scenarios designed to evaluate the effects of raising or lowering the variable settings.

- Review the ratio of false positives to “true” hits resulting in a SAR filing. Depository institution regulators have been saying since 2011 that this ratio is important in measuring the effectiveness of the program, according to Kathe Dunne, a seasoned consultant specializing in AML programs for banks and credit unions. Philip Lerma, Chief Risk and Compliance Officer of NetSpend (a leading provider of reloadable prepaid debit cards and related services) has focused on improving this ratio, partly because regulators are pushing for model validation and for sampling methodologies to check their thresholds. When he took over three years ago, the false positive rate in AML alerts was 1,000 to 1. Since then his team has lowered the ratio to 100 to 1.

---

17 Kathe Dunne, CAMS, in an interview with the author July 9, 2013
18 Philip Lerma, Chief Risk and Compliance Officer, NetSpend, in an address to the ACAMS Central Texas Chapter event on prepaid cards, 7/11/2013
OFAC testing
Office of Foreign Assets Control (OFAC) compliance is a strict-compliance law rather than risk-based, and the implementation of an OFAC system depends on many factors such as region, languages, nations, company size, and the appropriate levels of screening and vetting – even including such choices as to whether “weak” or “strong” AKAs (“also known as” names) are used for screening. Although the processes to test OFAC systems are similar to those listed above, OFAC is outside the scope of this paper. Testing that OFAC systems have been validated is an important part of an independent audit and is worthy of a separate research paper.

OCC Model Risk Management
The testing steps above conform to the increasingly important Office of the Comptroller of the Currency (OCC) Model Risk Management, which regulators are expecting financial institutions to understand and adhere to. The OCC 2011-12 Supervisory Guidance on Model Risk Management points out that models can impose costs, “…including the potential for adverse consequences from decisions based on models that are either incorrect or misused.” The OCC characterizes this potential for poor decisions, financial losses, and the resultant damage to reputation as “model risk.”

The ACAMS Webinar, Implementing an Automated BSA/AML Monitoring System — A Banker’s Perspective, presented August 22, 2012, advised, “The Regulators have been treating AML Systems as models and subjecting them to Risk Analysis Division (RAD) Scrutiny similar to credit risk models.”

While model risk validation is outside the independent auditor’s scope to validate the model, it is useful to determine whether the AML Compliance team or a qualified group, such as a dedicated model risk vetting (MRV) unit, has validated the model risk. This task requires technical competency and understanding of the source data and systems, the TMS, calculations and formulas used, and the business. This task can be substantial, depending on the complexity of the environment, the business, and the model, and the frequency of the task is risk-based. The independent AML auditor can audit the validation processes.

This includes the important step of checking the ratio of false positive alerts to positive alerts that result in SAR filings. The ratio is important for rating the effectiveness of the TMS and for justifying the staff to investigate alerts. Typically TMSs were generating thousands of alerts that compliance staff had to cull through before filing a SAR. Vendors and the institutions have increased the sophistication of the systems to reduce the noise of false positives. Insurers and TMS vendors have work ahead of them to achieve significant improvement in ratios in this industry.

Conclusions

The insurance industry is evolving its independent audit processes as it watches the states’ Insurance Commissioners and their examiners to see how the initial AML examination will be treated and FinCEN’s response to reports from the state examiners. While insurance is not yet being held to the same standards as banks, insurers benefit from testing the integrity and efficiency of their TMS and will be in a solid position for state or federal examinations.

In the current environment, the key to an effective and efficient independent audit of an insurance AML TMS is its testing for soundness and reasonableness. Testing employs the auditor’s business, audit and compliance skills. It tests the system by auditing the adequacy of system tests and the processes and the documentation supporting maintenance, data integrity validation, case management and reporting, appropriate tuning, and that the generation of alerts and reports as intended.

Meanwhile, insurers face a challenge in that the TMS model and data validation outlined here do not generally occur. Useful, incremental change can be achieved as independent auditors follow the testing methods proposed in this paper, document findings, and recommend model validation along with stringent processes for system testing, data validation and change management.