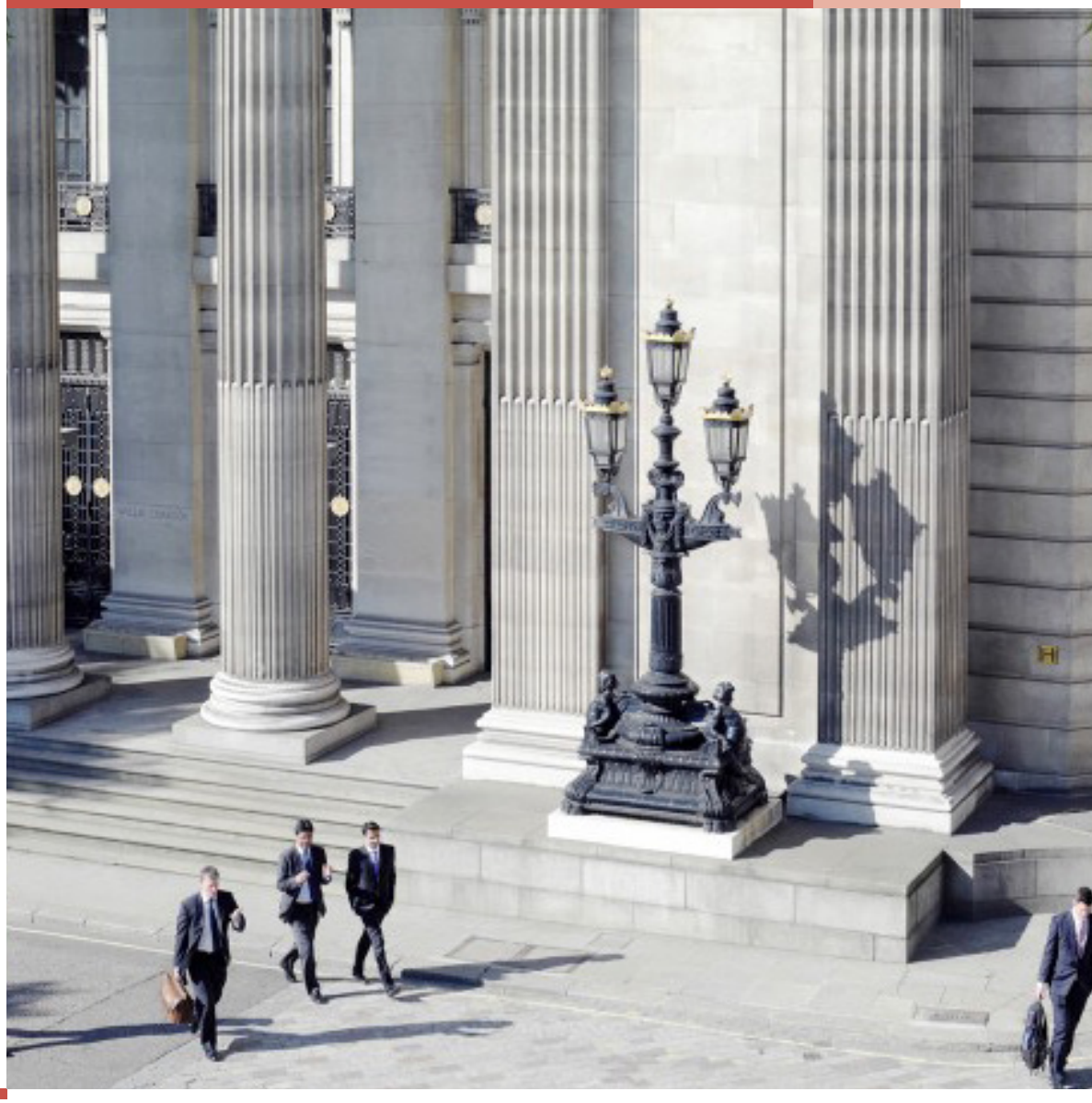
Avoiding the drift
Optimizing and maintaining AML surveillance programs

October 2013



pwc

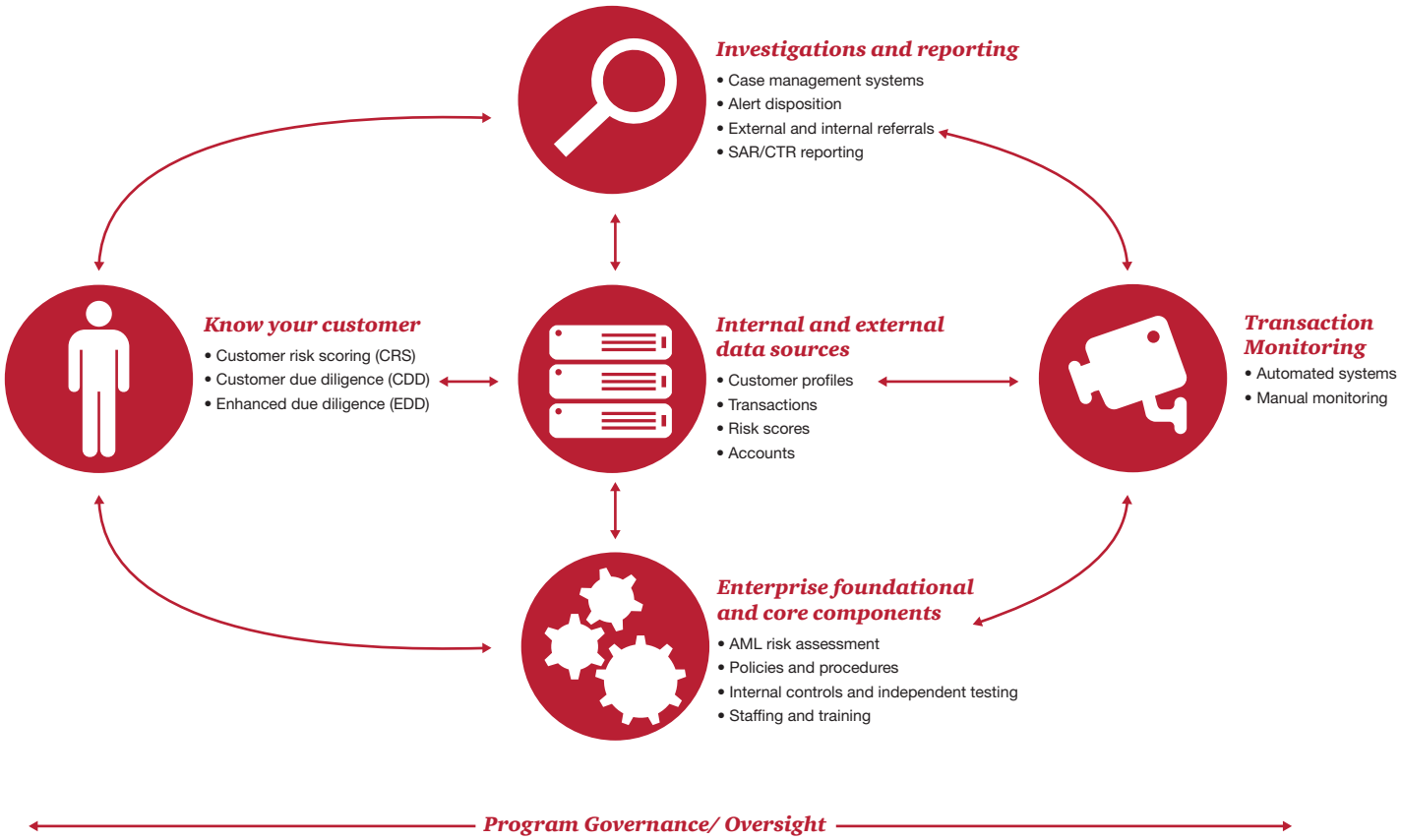
The heart of the matter

Without regular updating, AML systems can drift into inadvertent noncompliance.

Enacted in October 2001, the International Money Laundering Abatement and Financial Anti-Terrorism Act (an element of the USA PATRIOT Act) was designed to strengthen US measures to prevent, detect, and prosecute international money laundering and the financing of terrorism. The act built on existing requirements under the Bank Secrecy Act of 1970 (BSA), increasing criminal and civil penalties around money laundering and terrorist financing, widening the population of financial institutions to which anti–money laundering (AML) regulations apply, and significantly expanding the AML obligations incumbent upon those institutions.

Faced with these new requirements, financial sector companies poured billions into AML compliance efforts. They instituted new or upgraded due-diligence policies, procedures, and controls and built transaction surveillance systems able to detect patterns indicative of criminal money laundering and terrorist financing. They created new departments to manage these systems and conduct investigations and hired new compliance officers to oversee them. They instituted training programs to mainstream and maintain AML practices across the enterprise and began conducting regular independent audits to test their controls.

Bank Secrecy Act/Anti-Money Laundering Program Overview



Yet despite this enormous investment in systems, training, and assurance, the AML ship has lately begun springing leaks.

Since 2008, US regulators have imposed substantial fines and issued a large number of cease-and-desist consent orders against US and foreign banks, citing lax AML compliance. Between 2008 and early 2013, the Federal Reserve issued 113 enforcement actions relating to compliance with the BSA and with economic sanctions administered by the Treasury's Office of Foreign Assets Control (OFAC).[1]

Why, with all the efforts put into AML across the financial services community, are these problems occurring? In some instances, banks have been aware of specific AML risks but failed to take corrective action. One of the banks noted above, for example, failed to address significant AML compliance problems in its operations, which allowed drug cartels to launder—approximately $881 million. While the magnitude of both the failure and the resulting $1.9 billion fine make this a particularly marquee-worthy example, it serves as a warning to all financial institutions: A company need not intend to launder money to be found guilty of laundering money. "Willful blindness" is enough—and that includes failing to maintain adequate systems, oversight, and controls.

The more complex a system, the more opportunities for breakdown, a fact that leaves the financial industry vulnerable to AML compliance risk. At many financial institutions, inadequate attention and resources have been dedicated to maintaining and sustaining the core components of AML programs that may now have been in place for more than a decade, leading to gaps in AML compliance. We call this gradual process of inadvertent noncompliance "AML drift," and it occurs because AML systems are reliant on numerous variables across the organization, including where transaction information is stored, changes to financial products and services (and the introduction of new products and services), and changes in customer behavior. To account for changing conditions, AML systems need to be constantly monitored, updated, maintained, and repaired. When they're not, drift is inevitable.

Drift happens in three places: processes and updates, technology, and organization. To protect against drift and keep their AML programs up to date, companies need to do better, more data-based testing. They need to think about the type of metrics they're using to monitor their program. They need to uplift the technology they use for monitoring. And they need to make sure their organization is aligned correctly to ensure that AML programs are kept updated and functioning at peak efficiency. If companies get this right, they will protect themselves not only from regulatory fine and censure, but from the potentially costlier reputational risks that could follow.

1 "Anti-Money Laundering and the Bank Secrecy Act," testimony by Federal Reserve Board Governor Jerome H. Powell before the Committee on Banking, Housing, and Urban Affairs, US Senate, Washington, DC (March 7, 2013); http://www.federalreserve.gov/newsevents/testimony/powell20130307a.htm.

An in-depth discussion

Process failure can occur at any point along the AML lifecycle.

How AML programs work… and how they can break down

All anti–money laundering programs share similar structures and processes:

1. **Know your customer procedures** are the tools that help financial institutions gain a detailed understanding of their customers, including their identity, citizenship status, occupation, source of funds, volume and type of expected activity, countries with which they do business, etc. By collecting this information and keeping it continually updated via transaction monitoring, companies are able to assign their customers into high-, medium-, and low-risk categories and apply further due-diligence as appropriate.

2. **Surveillance processes** allow banks to monitor for money laundering typologies: people moving money inside and outside the bank very quickly; a pattern of "structuring," in which a customer continually makes deposits just below the reporting threshold; a single beneficiary receiving money from multiple originators; customers who are depositing large sums and making wire transfers to high-risk countries; and so on. Surveillance also typically includes Office of Foreign Assets Control (OFAC) screening, in which bank customers' names are compared against lists of known terrorists and other high-risk individuals.

3. **Investigations and reporting efforts** are based on KYC and surveillance data. Once a customer or transaction has been flagged, it goes through a case management workflow to manually investigate the cases and file suspicious activity reports (SARs) to the Treasury Department's Financial Crimes Enforcement Network (FinCEN).

4. **Enterprise foundational and core components** underlie the entire AML effort, assuring that the institution has conducted a risk assessment to identify money-laundering and terrorist financing exposures across its products, services, customers, and geographic locations; understands how money-laundering and terrorist financing typologies apply across those products, services, and geographies; has put the appropriate AML policies, procedures, and training mechanisms in place; and runs regular audits to test its AML program controls.

Breakdowns in the process

AML drift can occur in three key areas:

1. **Processes and updates.** To stay effective and in compliance, an AML program must be constantly updated to keep up with changing regulations and new financial products. If your company is launching a new product, you have to be sure that product is properly accounted for in your AML monitoring system. If you're seeing other companies hit with consent orders or fines due to a particular AML deficiency or issue, you must have processes in place to evaluate that issue within your own environment and identify any changes that might be needed to your systems, processes, and controls.

2. **Technology.** To prevent breakdowns in AML monitoring, a company's IT change management process must track all systems changes that have the potential to affect AML monitoring. For example, in a financial institution's core banking system, processes must be in place to alert a company's AML compliance function if a new transaction code is added or a change is made to how an existing transaction code works. If such a mechanism is not in place, the AML system will no longer function as intended, because the data the system is receiving has been changed upstream.

3. **Organization.** Often, drift occurs due to a lack of accountability and ownership over AML issues: Operations thinks they're IT's job, IT thinks they're Compliance's job, Compliance thinks they're internal audit's job. The lack of clear ownership rules across and among the silos leads to holes going unplugged, and thus to drift.

Key AML control questions

Know your customer

- Are we confident that all our customers go through a CDD/ EDD process?
- How are our files reviewed for quality assurance?
- What are our policies around high-risk customers?
- Are our KYC questionnaires regularly updated to industry standards? How is this done?
- How do we score customers?
- How often is our scoring model validated?

Surveillance

- Do we have the right scenarios?
- Are the scenarios optimized?
- Is all the data monitored?
- Is the reference data accurate?
- How do we handle known issues with data and monitoring?

Investigations and reporting

- Are we investigating everything generated through our AML processes?
- What offshore risks exist?
- Are we filing SARs for all suspicious activities that meet reporting thresholds?
- Is the data coming together from different parts of the firm?
- Are our investigators properly and fully trained?

Enterprise foundational and core components

- Are our risk assessment questions consistent and correct?
- Do we capture everything in our risk assessment?
- Are our people compliant in training?
- Is testing independent and complete?

What this means for your business

Methods and techniques to avoid AML drift

Avoiding the drift means avoiding damage: to your company, its reputation, and its bottom line, whether from lost business, costs associated with look-back efforts and damage control, or fines due to noncompliance with regulatory statutes.

In the face of evolving money laundering and terrorist funding typologies, financial institutions need to assure the continued integrity of their AML protocols by promoting clarity in their standards, metrics, tools, and organizational alignment. They need to implement independent testing of every aspect of their monitoring systems, from the quality and completeness of source data to the productivity of existing and potential scenarios. They need to continuously monitor their AML controls, making sure thresholds and scenarios are up-to-date and that metrics are in place to detect potential areas of drift. They need to leverage technology to help prevent drift—for example, by developing automated tools for rapid decision making and issue identification, and by employing workflow tools to support documentation of AML processes, procedures, and methodologies. And they need to make sure their whole organization is aligned to promote AML compliance, with clearly delineated responsibilities, lines of reporting, and training. The following are quick hit areas to help "avoid the drift."

Source-to-surveillance testing and model validation.

"Source-to-surveillance testing" is to thoroughly assess all components of an AML monitoring process, from the quality and completeness of source system data to the effectiveness of detection scenarios. The approach has four primary components:

- **Data sourcing analysis.** Reviews data fed from the various source systems (e.g., core banking/ deposits, commercial lending origination, residential mortgage servicing, etc.) for potential gaps and quality issues that may impact AML monitoring.
- **Data quality analysis.** Reviews the completeness, quality, and integrity of data elements used by existing and potential scenarios.
- **Mapping and transformation.** Analyzes logic or transformation from source systems to the monitoring systems that are critical to surveillance efforts.
- **Scenario testing.** Evaluates the productivity and the reasonableness of existing and potential scenarios and tests the logic behind them.

Optimization and metrics

To enable continuous and effective monitoring of AML controls, companies must make sure their

thresholds and scenarios are up-to-date and that they employ the correct metrics. Using techniques and tools such as productivity analysis and key performance indicators can help companies optimize and fine-tune their scenarios and metrics to promote more effective alerts, with fewer false positives. Optimization efforts should include:

- **Scenario evaluation**. Uses understanding of current industry practices and circumstances, SARs issues, and investigation feedback to evaluate the effectiveness of scenarios.
- **Segmentation analysis.** Utilizes behavioral analysis to ensure customers are alerting appropriately.
- **Threshold tuning.** Tests and sets thresholds against segments.
- **Ongoing metrics.** Develops metrics to use on an ongoing basis. Monitoring not only the metrics themselves but *trends* within the metrics can help detect potential areas of drift.

Tools and utilities

Having the right IT tools and utilities is essential to a well-functioning AML monitoring and compliance program, and to managing drift. Workflow tools, for instance, can support documentation. Visualization tools allow the creation of accurate metrics. Suspicious activity detection tools allow for statistical analysis of historical transaction data and alert output, giving institutions the means to identify trends and patterns and better determine which behaviors fall outside an acceptable range. This analysis can also be a first step in selecting appropriate rules and thresholds and later reassessing the monitored behaviors and thresholds over time—determining correlations and trends between productive and non-productive alerts and allowing refinements that better target potentially suspicious activity.

Vital tools and utilities include:

- **Visual analytics tools (e.g., Spotfire, Tableau, Qlikview).** Visual analytics tools create dashboards and other visual representations of data to assist in identifying patterns, anomalies, and transaction trends. Such tools are used to create executive-level dashboards and threshold tuning exercises.
- **Data manipulation and statistical analysis tools (e.g., SAS).** These tools can enable processes such as time series modeling, vector auto regressions, and principal component analysis on transactional data. They're used for segmentation analysis and to create predictive models for transactions.

- **Data warehousing/ETL tools (e.g., Oracle, Teradata, Informatica).** These tools handle the loading, transformation, normalization and storage of large data sets.

- **Automated transaction monitoring tools (e.g., Actimize, Mantas, Norkom).** TM systems are designed to detect and flag patterns of predefined suspicious transactions for investigation.

Organizational models and lines of defense

Clarity in the structure of responsibilities is central to avoiding AML drift: making sure the organization is aligned, responsibilities are clear, people throughout the different silos know what they're responsible for, and everyone is clear not only about what they're doing but about what the other functions are doing. Central to the process are:

- **Operations.** Runs and implements the business as usual.

- **Risk management.** Understands and tests controls.

- **Compliance.** Advises and defines the program including policy and governance.

- **Project management.** Manages changes, upgrades, and continuous improvements.

- **Technology.** Manages core technical components and change control.

- **Internal audit.** Forms the last line of defense by testing controls.

The cost of noncompliance

While the costs of maintaining and updating AML systems can be high, the costs of noncompliance can be even greater and longer-lasting, and include monetary losses (fines, legal costs, etc.), reputational damage related to loss of customer and investor confidence (and potentially leading to concentration risks), and operational risk, with legal actions such as cease-and-desist orders and consent orders taking a bite out of the bank's core businesses.

In an ever-more-complex, globalized business environment, with regulators stepping up their game and the public increasingly tuned in to compliance failures and their repercussions, financial institutions need to live in the moment from an AML perspective. Fed with the right information and managed with updated controls to ensure its continuing effectiveness, AML monitoring needs to become a living organism, able to protect the business from risks across all customers, products, geographies, and regulatory regimes.

www.pwc.com

To have a deeper conversation about how AML drift may affect your business, please contact:

John Sabatini
Advanced Risk and
Compliance Analytics
Leader
PricewaterhouseCoopers
(646) 471-0335
john.a.sabatini@us.pwc.com

David Choi
Advanced Risk and
Compliance Analytics
Principal
PricewaterhouseCoopers
(646) 471-6748
david.d.choi@us.pwc.com

Vikas Agarwal
Advanced Risk and
Compliance Analytics
Managing Director
PricewaterhouseCoopers
(646) 471-7958
vikas.k.agarwal@us.pwc.com

NY-14-0150