

Financial Institutions Point of View

Best Practices for AML Compliance



As the war on terrorism continues, financial institutions are under intense regulatory pressure to enhance their anti-money-laundering (AML) programs. The first step is a comprehensive risk assessment that evaluates an institution's money-laundering exposure based on its unique risk profile.

Summary

A key strategy in America's war on terrorism is the elimination of terrorists' financial supply lines. Financial institutions play a critical role in this effort and to wage an effective AML campaign, an institution must first gather intelligence on suspected enemy resources and activities.

The analogy between AML and war is appropriate. For example, the military may sometimes utilize carpet or saturation techniques to strike enemy targets. In many cases, however, such indiscriminate tactics succeed only in wasting resources and resulting in collateral damage. It is far more effective and efficient to identify the most significant threats and then launch precision strikes designed to pinpoint those targets.

The same principles apply to financial combat. By conducting a comprehensive risk assessment, a financial institution can gather the intelligence it needs to focus its AML efforts on high-risk customers, products and activities. This strategy enables the institution to allocate its AML investment effectively, avoid wasting resources and minimize the possibility of collateral damage to its relationships with low-risk customers.

A risk assessment also provides an institution with the ammunition it needs to demonstrate to regulators that its AML program is effective. Today, regulators follow a risk-based approach to compliance. As a result, financial institutions must be prepared to convincingly demonstrate that their AML programs are tailored to their risk profiles.

One of the most effective ways to evaluate an institution's money laundering risk is to analyze its existing risk factors identified in relation to its unique AML risk profile and then review them against a framework of AML best practices.

Trends

The *Bank Secrecy Act* (BSA) is the federal government's primary anti-money laundering law. Since its passage, the BSA has been amended and revised numerous times in response to increasingly sophisticated criminal practices and technologies. Major revisions to BSA were implemented following the terrorist attacks of September 11, 2001 (9/11). Prompted by the tragedy of 9/11 and empowered by the resulting changes to the BSA, law enforcement agencies and bank regulators shifted their AML focus from traditional criminal activities to concentrate on terrorist organizations. Today, the BSA's anti-money-laundering regulations require financial institutions to monitor customer behavior, maintain records of certain types of transactions, and file reports with the government. Required reports include "currency transaction reports" (CTRs) describing cash transactions in excess of \$10,000, and "suspicious activity reports" (SARs) describing activities perceived by the institution to be suspicious or out of the ordinary from a customer's usual pattern of activity.

To provide law enforcement with more effective weapons against terrorist financing activities, the *USA PATRIOT Act* made several changes to the BSA. Section 314, for example, requires information sharing between financial institutions and law enforcement through the medium of the Financial Crimes Enforcement Network (FinCEN). Section 326 requires financial institutions to:

- Implement a written, risk-based customer identification program (“CIP”);
- Maintain records that provide specific categories of customer information and describe methods used to verify customers’ identities; and
- Compare the names of new customers against government lists of known or suspected terrorists or terrorist organizations.

Terrorism concerns have made BSA compliance a top examination priority for regulators. The Bush administration has reinforced this priority by progressively boosting FinCEN’s power to oversee and support regulators’ examination functions. Today, FinCEN works vigorously with regulators to emphasize risk-based compliance procedures. Compliance with this risk-based approach requires that institutions do far more than simply implement systems to file SARs and CTRs. Now, the government expects financial institutions to actively monitor high-risk customers and activities in a proactive effort to detect and prevent money laundering.

Gaps

Most financial institutions have AML programs in place, and many have conducted risk assessments. Often, however, institutions’ AML policies and procedures are insufficient to meet regulators’ demanding expectations. A number of reasons may account for this shortfall, yet common explanations include weak internal controls, inadequate training of personnel, and insufficient independent testing of an institution’s compliance program.

Compliance gaps often result when institutions apply a cookie-cutter approach to AML risk assessment and program design. To satisfy regulatory scrutiny, an institution’s AML program must be customized to fit the institution’s particular blend of assets, customers, geographic locations, and products and services. A large, regional institution in the Southeast, for example, may exhibit relatively low overall risk, while its branch office in Washington, D.C., may represent a high-risk pocket that must be specifically and individually addressed.

Challenges

Financial institutions are faced with two critical, sometimes conflicting, challenges. On the one hand, they must develop and implement thorough AML compliance programs that satisfy banking regulators and make efficient use of limited resources. At the same time, they must avoid behaviors of the rigorous, customer-focused due diligence, required by those same AML programs, that damage customer relationships.

An effective, well-designed risk assessment can help a financial institution meet both of these challenges. By proactively demonstrating to examiners that its AML policies, procedures and technologies are tailored to its specific risk profiles, an institution can avoid the more intrusive and costly procedures that examiners often impose on programs they find inadequate. At the same time, by concentrating its most intense due diligence activities on high-risk customers, products and services, the institution can ensure that its compliance investment is leveraged to concentrate on the point of greatest vulnerability

and to minimize the potential impact of strenuous due diligence on low-risk customers.

Solutions

A financial institution aiming to build an effective AML program that will meet examiner standards should take a systematic approach to risk assessment. This three-step approach should include the following key components:

Step One — A **Quantitative analysis** of an institution's specific risk factors based on its asset size, geographic location, customer base and the types of products and services it offers;

Step Two — A **Qualitative analysis** of the controls, capabilities, technologies and people resources the institution has in place to mitigate the risks identified during Step One; and

Step Three — A **Gap analysis** that identifies areas in which the institution's controls, capabilities, technologies or staff resources are inadequate to support an effective AML program.

To identify gaps in Step Three, an institution must know how its compliance program *should be* performing. Comparing its existing program to a visual representation of a best practices AML program, a financial institution can create an accurate, comprehensive road map to successful AML compliance.

The ideal approach - a *closed-loop* approach - is centered on two key activities: (1) sharing of key customer information throughout the entire organization, not just the banking centers; and (2) building effective feedback mechanisms among all AML processes and systems to remove silos of information. Only by gathering customer information from all sources and then making it available to the entire organization can an institution develop an accurate picture of its money-laundering and terrorist-financing risks.

Key features or elements of a sound and comprehensive AML program assessment include:

New account opening procedures. The information gathering process begins when a customer opens a new account. The *USA PATRIOT Act's* CIP provisions require the institution to verify the customer's identification and address, compare the customer against lists of suspected terrorists and politically exposed persons (such as current or former senior foreign officials), and determine whether the customer meets the criteria for a money service business (MSB). Many customers use MSBs to wire money overseas. As a result, MSBs represent a potential for increased risk because they can be used as a mechanism for terrorist-financing or money-laundering activities.

Sustained customer-identification procedures. An institution's customer-identification responsibilities do not end after an account is opened. Dynamic know-your-customer (KYC) procedures allow the institution to maintain an ongoing, real-time customer profile. KYC information is gathered at both the customer and the account levels. The type and amount of information collected depends on the institution's risk profile. Consequently, each institution's KYC program is different. At the customer level, the institution collects essential information, such as an individual account holder's country of citizenship or a business account's primary industry. At the account level, the institution collects information on expected and actual activity patterns, such as funds wires and trading

partners.

Institutions should develop a core set of questions to ask new customers. These may include queries such as: "Do you cash checks for more than \$1,000?" "Do you intend to use our wire services in conjunction with the account you are opening?" and "If so, do you plan to wire money overseas?" Customer answers to these questions may increase or decrease individual risk ratings, and the information collected provides a well-informed basis for future transaction monitoring.

Customer risk rating. Using new account data and KYC information, the institution should assign the customer an *objective* risk score. The exact methods and scope of scoring are based on the institution's risk profile, but common requirements include:

- The ability to set multiple risk thresholds to categorize customers into low, medium or high risk categories;
- The ability to easily change risk factors based on new and changing requirements; and
- The ability for the compliance department to monitor a customer's risk score over time.

Enhanced Due Diligence. Based on the customer's risk rating, the institution may reject high-risk customers or it may conduct additional enhanced due diligence. This due diligence may include prompting for additional information at the time the account is opened or performing additional background or business checks after the account is opened but before funds are released. High-risk customers who are accepted may be monitored more closely.

Transaction monitoring and reporting. As transactions occur, the institution should filter and analyze them for unusual or suspicious activity. Personnel should be trained to recognize suspicious activity and, when such activity is identified, to follow up on a basis of effective established procedures. Transaction monitoring systems that incorporate reliable algorithms should be implemented to detect unusual or suspicious activity based on statistical analysis and other advanced analytical capabilities.

The institution is required to file CTRs that report cash transactions in excess of \$10,000. Using a case management system, the institution should investigate and document any unusual activities and should file SARs describing any activities deemed to be suspicious.

Record-keeping. CIP regulations require institutions to retain customer identification documentation and non-documentary information for five years after an account is closed. Whenever customer profile information is electronically updated, the institution must log the changes made and must record the source and date of the revision. Good record-keeping will provide a due diligence audit trail that enhances the institution's case management and investigative capabilities.

Customer vetting. In addition to new account procedures, best practices also demand that a financial institution conducts a thorough, risk-based examination of its existing customer population and applies its enhanced due diligence processes to high-risk customers. This approach will enable the institution to screen established customers whose accounts were activated prior to the implementation of updated and more rigorous identification procedures. It will also allow the institution to identify newer customers

whose actual activities deviate in meaningful ways from their initial account start-up profiles.

Data store for single customer view. An integrated and unified view of the customer is critical to each of the AML best practices described above. The institution must be able to extract and filter information from all available sources. It should also have the capacity to make the resulting data available to appropriately authorized officials through a common user interface. By compiling and integrating information about a customer's accounts and transactions, the institution will be able to identify high-risk customers, forecast and monitor future activities, recognize anomalous or suspicious behavior, and respond quickly and thoroughly to requests for information.

A single customer view will also provide important marketing benefits, enabling the institution to identify gaps in its customer relationships and develop strategies for closing those gaps. In more technologically sophisticated institutions, this information can be made available in real time using enterprise application integration (EAI) technology.

Foundational structure. The components of a best practices AML program should be supported by four critically important foundational capabilities. These include:

- The institution's AML risk profile, based on products, geography, customer demographics and other factors.
- A demonstrated ability to plan and execute AML projects, through a program office if necessary.
- Training at all levels — tellers to board members — in conjunction with effective self-testing of the institution's AML controls.
- Up-to-date written policies and procedures.

Conclusion

The key to an effective AML program is risk assessment; and the key to competent risk assessment is a clear understanding of where an institution's program is today and where it needs to be. This model provides institutions with best practices benchmarks they can use to construct a road map to successful and sustained AML compliance.

Contact Information

Greg Hahn can be reached at 616.752.4223 or ghahn@crowechizek.com.

Crowe Chizek and Company LLC is a member of Horwath International Association, a Swiss Association (Horwath). Each member firm of Horwath is a separate and independent legal entity. Accountancy services in the State of California are rendered by Crowe Chizek and Company LLP, which is not a member of Horwath. This material is for informational purposes only and should not be construed as financial or legal advice. Please seek guidance specific to your organization from qualified advisors in your jurisdiction.