



Anti-Money Laundering Compliance Survey



Executive Summary

Complying with the new requirements of the USA PATRIOT Act, especially for financial services institutions that have been given new anti-money laundering (AML) responsibilities for the first time, will require a fundamental change of outlook and the acquisition of new skills by the legal and compliance function.

Meeting these new AML requirements may also create significant operational challenges for financial services institutions. In addition to regulatory expertise, the compliance function now has to acquire a whole set of new skills in such areas as the design of business processes, employee training, and program management. The dramatically increased volumes of transactions that must be reviewed demand that institutions rely more heavily on IT systems to automate routine reviews and identify items that require more detailed analysis and evaluation. The size of the workload may require many institutions to adopt a new philosophy, seeking to strike the proper balance between speed and effectiveness in reviewing transactions. In short, the new environment requires that financial institutions “operationalize” AML compliance.

Financial institutions will also need to determine how to best organize AML compliance within their firms. For example, they should consider having AML compliance report to a senior executive since effective compliance requires key decisions on organization-wide issues such as technology and training.

Most securities, asset management, and insurance firms are only now confronting these issues as they begin to assume their new AML responsibilities. While banks have had AML responsibilities for many years, they are also taking a new look at their compliance function in light of expanded AML requirements.

While each institution must design its compliance function to be compatible with its business model and corporate culture, the following are some of the questions that most firms will need to ask themselves:

Organization

- Will a qualified senior executive be given oversight responsibility for AML compliance?
- Will there be a legal and compliance function dedicated to AML compliance or will existing divisions manage it?

Technology

- Will AML technology be integrated in the IT function or managed separately?
- Will the institution acquire vendor applications or develop its AML applications internally?

Training

- Will AML training be customized to the specific needs of business units and support functions based on their specific AML risks?
- How will the content of AML training be determined?
- How will the effectiveness of AML training be assessed?

Testing

- Will independent AML testing be supported by business unit self-assessment and compliance reviews to provide a comprehensive monitoring process?

Risk-rating Methodology

- Will a customer risk-rating methodology be used in conjunction with transaction analysis to assist in identifying suspicious activity?

Enhanced Due Diligence

- Are there clearly defined categories of customers for whom enhanced due diligence (EDD) is necessary?
- Have the activities that must be performed to meet EDD requirements been specified?
- Will a structure such as a financial intelligence unit be established to assist with meeting EDD requirements, identifying suspicious activity, and conducting investigations of individual customers, potential customers, or transactions?

While these questions are relevant to most institutions, financial services institutions that are assuming AML compliance responsibilities for the first time must confront additional issues specific to their industry. For example, insurance institutions will need to consider conducting risk assessments to determine the order in which they will develop and implement AML programs for their business units when regulations are issued for Section 352 and Section 326.

Asset management institutions also face unique issues. If an asset management institution has outsourced transfer agency to a third-party, what oversight model will it employ? Does the transfer agency system have technology that is adequate to handle AML compliance or will additional technology be required? Mutual fund or asset management complexes that are part of larger financial services institutions will need to evaluate whether they can leverage the infrastructure of their corporate parent in such areas as legal, compliance, technology, and training.

To gain insight into these challenges that financial services institutions face in complying with AML requirements and the steps they are taking to meet them, Deloitte & Touche conducted a survey of 167 senior financial services executives with AML responsibilities.

Principal Findings

Key Challenges

- *Establishing appropriate business processes* was rated as the most significant issue in meeting the requirements of the Act, with 92% of executives rating it as very or extremely significant.
- *Monitoring AML regulations in the United States* was rated as a very or extremely significant compliance issue by 91% of executives, while training employees received this rating from 86% of executives.

Suspicious Activity Reports (SARs)

- Roughly half of executives reported that their firm filed two or fewer SARs on average each month. However, 14% of executives said that their institution filed an average of 25 or more SARs each month.
- Forty percent of executives said that their number of SARs filed had increased over the past six months.

Testing

- More than 80% of executives reported that their institution had tested its AML program, and two-thirds said that it uses a centralized approach to testing.
- Testing will be conducted only once or twice in the coming year at their institution according to 86% of executives. Yet, almost one-fifth of banking executives said that their institution will conduct testing five or more times in the coming year.

Training

- More than 90% of executives said that their institution provides AML training.
- Almost three-quarters of executives identified the compliance department as the group that designs and conducts AML training.

Technology

- Sixty-two percent of executives said that their institution used a vendor application to automate Office of Foreign Assets Control (OFAC) screening, an additional 21% said that their institution used both a vendor application and software developed internally, and 8% said that they relied on software developed internally. Surprisingly, 10% of executives reported that their institution didn't use software for OFAC screening.
- For AML transaction monitoring, each of the following approaches was cited by roughly one-quarter of executives—a vendor application, proprietary software, and a combination of both a vendor application and proprietary software.

Each of these findings is discussed in more detail in the following sections. >>>

Survey Results

What challenges do financial services institutions face in complying with the Act and other anti-money laundering requirements and how are they responding? To answer this question, Deloitte & Touche surveyed 167 senior executives at U.S. banking, securities, asset management, and insurance institutions on the approaches they are taking to AML.

The terrorist attacks of September 11, 2001 led to a heightened concern over money laundering, especially by groups involved in monitoring terrorism. These concerns were the principal motivation for the passage of the Act and other new regulations that expanded AML requirements for financial services institutions. In particular, the Act for the first time placed a number of AML responsibilities, such as filing Suspicious Activity Reports (SARs), on securities, asset management, and insurance institutions.

The survey asked executives about their most important issues in complying with the Act and then probed about their institution's experience in four specific areas: suspicious activity reports, training, testing, and technology. The survey findings on each of these topics are detailed in the sections below.

Key Challenges

Executives rate establishing appropriate business processes, monitoring U.S. AML regulations, and people-related issues as most important in complying with the Act. Although technology was a significant concern, it was seen as less important than these top-rated issues. While critical in enabling AML compliance, technology depends on an institution's business processes and people to be effective.

Establishing appropriate business processes was rated as very or extremely significant to compliance with the Act by 92% of executives. (See Exhibit 1.) Executives also rated a related issue highly, with 81% saying that assigning clear responsibilities was very or extremely significant to successful compliance.

With new AML regulations being issued, *monitoring AML regulations in the United States* was the second highest rated issue, considered very or extremely significant by 91% of executives.

People-related issues were also rated highly. Eighty-six percent of executives rated *training employees* as very or extremely significant, while 78% gave similar ratings to *securing adequate attention from senior management* and to *gaining employee commitment*.

Deloitte & Touche's experience indicates that the commitment of a firm's leadership—both senior management and the board of directors—to its AML program is essential. Beyond legal requirements, the board of directors and senior management need to make key decisions that cut across traditional functional boundaries. In addition, the active involvement of senior management demonstrates to middle managers and lower-

Exhibit 1 | Significance of Issues in Complying with USA PATRIOT Act

Percent of Executives Rating Issue as Very or Extremely Significant



level staff the importance that the institution places on AML compliance. Financial services institutions that have experienced regulatory problems with their AML programs often find that one reason is a lack of attention and commitment by senior management and the board of directors.

Although rated highly, technology issues were seen as somewhat less important to compliance than issues affecting business processes and people. Approximately three-quarters of the executives rated *deploying the right technology* as a very or extremely significant issue.

What is clear is that addressing all these issues will cost money. Three-quarters of executives said that spending would increase in the next 12 months in the areas where they have AML responsibilities. Deloitte & Touche's AML experience with clients suggests the areas that should be considered for additional spending include restructuring business processes, increased staffing, employee training, purchasing or developing new technology, and enhanced monitoring of regulatory developments.

Suspicious Activity Reports

Eighty-six percent of executives said that their institution was required to file Suspicious Activity Reports (SARs). While banks have been required to file SARs for several years, this only became a requirement for broker-dealers on January 1, 2003 and the regulations are still being developed for asset management and life insurance institutions. Yet many firms that are not yet required to file SARs still file to minimize the possibility that they will inadvertently conduct business with an individual engaged in illegal activity. Sixty-one percent of executives at institutions not required to file SARs said that they had chosen to file voluntarily.

Half the executives reported that their institution filed on average two or fewer SARs per month over the last six months. (See Exhibit 2.) In contrast, 14% of executives said that their institution filed an average of 25 or more SARs each month. These higher volumes of SAR filings were more common in banks—28% of banking executives said that their institution filed on average of 25 or more SARs each month.

The number of SAR filings is increasing for many institutions. Almost 40% of executives said that the number of SAR filings by their institution had increased over the last six months, and 55% of banking executives reported volumes of SARs were increasing. (See Exhibit 3.) It is quite possible that this increase in SAR filings has been due to increased vigilance rather than an actual increase in suspicious activity since firms now have the benefit of better monitoring systems and improved technology.

Exhibit 2 | Average Number of Monthly SARs Filings

Percent of Executives;

Base = Firms Filing SARs for Six Months or Longer

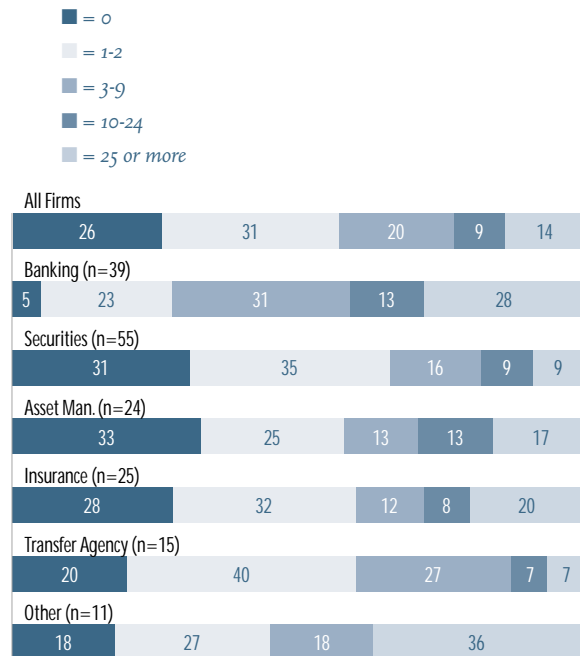
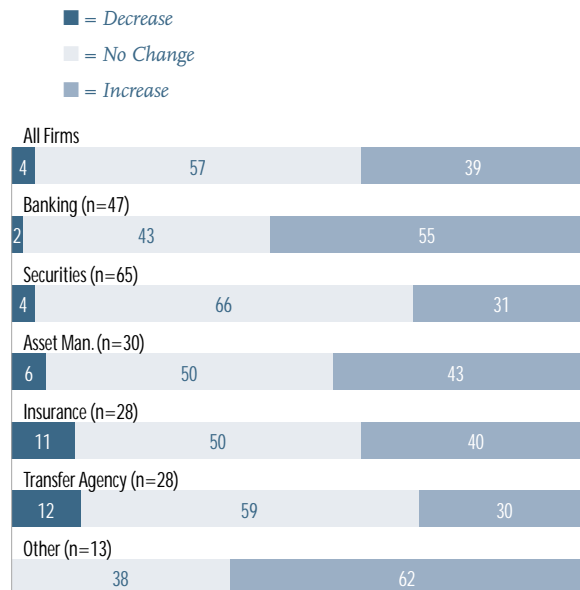


Exhibit 3 | Change in Number of SARs Filings Over Past Six Months

Percent of Executives

Base = Firms Filing SARs for Six Months or Longer



Testing

Eighty-three percent of executives reported that their institution had tested its AML program, and most institutions rely on internal personnel for testing. Fifty-seven percent of executives said that testing was conducted by internal audit, compared to only 17% that reported testing being handled by a third-party vendor.

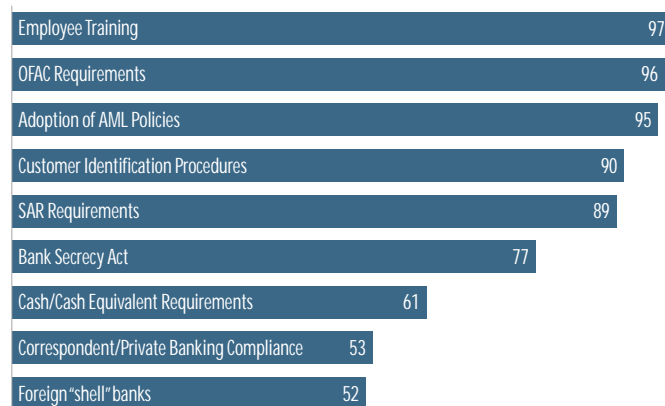
There was also consensus on employing a centralized approach in testing. Two-thirds of executives said that their institution managed AML testing centrally, rather than allowing it to be handled by individual business units.

More than four-fifths of the executives said that AML testing would be conducted once or twice in the next 12 months. While only 6% of all executives said that their institution plans to conduct AML testing five or more times in that period, almost one-fifth of banking executives said that their institution followed this more aggressive testing schedule.

When it comes to the issues addressed in their institution's AML testing, almost all executives cited employee-training requirements under Section 352 of the Act, compliance with OFAC requirements, and adoption of AML policies and procedures required by Section 352. (See Exhibit 4.) Roughly 90% of executives also cited as elements of their AML testing program compliance with suspicious activity reporting requirements and verification of customer identification procedures under Section 326, which is still being implemented fully.

Exhibit 4 | Issues Addressed in AML Testing

Percent of Executives

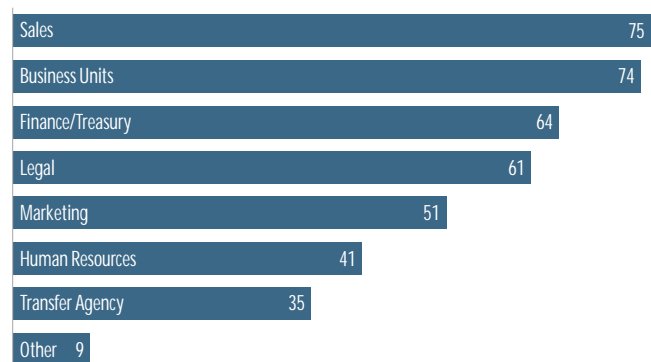


Training

Training of employees, officers, and directors is essential to a successful AML program. Ninety-three percent of executives said that their institution provides AML training. The individuals in contact with the customer are most likely to receive training—sales and business units were cited by three-quarters of executives as groups that received AML training. Individuals in some central functions are also likely to receive training, with more than half of executives naming finance/treasury, legal, and marketing as additional areas whose employees receive AML training. In addition to training internal staff, investment management institutions that use outside transfer agencies will want to ensure that these critical third parties receive adequate training. Many institutions provide basic training on AML requirements to a wide range of employees and then supplement this with more targeted, customized training that is keyed to the specific business activities and is closely tied to the institution's specific policies and business procedures. (See Exhibit 5.)

Exhibit 5 | Groups Receiving AML Training

Percent of Executives Citing Each Group



Almost three-quarters of executives said that the compliance department was responsible for designing and conducting AML training. In many institutions, employee training is a new responsibility that the compliance department has had to assume to comply with AML requirements. In addition to the expanded role for the compliance department, this is another area where senior management involvement is critical. Senior management needs to not only review and approve the course content, but also communicate to employees the importance of committing the time to be trained.

Traditional classroom training is still the most popular approach, cited by 70% of executives. However, roughly half the executives said that their institution used self-directed, computer-assisted training and another half named online training methods, while 22% use webcasts for training. In particular, large institutions with employees who are geographically dispersed have found that combining classroom training with online and computer-assisted training is more efficient. Such institutions often use classrooms for general AML training and then supplement this with computer-based training methods on issues specific to particular business units or lines of business.

Technology

The use of software to automate AML reviews is increasingly important as regulatory requirements expand and transaction volumes increase. The use of vendor applications to automate AML tasks appears to be more advanced in the area of OFAC screening than in AML transaction monitoring.

The difference between OFAC screening and AML transaction monitoring explains this divergence. OFAC screening is more cut-and-dried—an individual or group either is on the OFAC list or not. AML transaction monitoring, on the other hand, requires interpretation and judgment. These differences are reflected in the cost of vendor applications. Applications for OFAC screening can cost less than \$10,000, while the bill for AML transaction monitoring applications can be between \$250,000 and \$1 million.

In the area of OFAC screening, more than 60% of executives said that their institution uses a vendor application for OFAC screening, another 21% said that it combines a vendor application with software developed internally and 8% develop software internally. Surprisingly, 10% of executives reported that their institution doesn't use any software for OFAC screening.

The approaches taken by institutions in AML transaction monitoring varied much more widely. Each of the following approaches was cited by roughly one quarter of executives—use of a vendor application (24%), use of software developed internally (24%), and a combination of these two approaches (23%). Yet 29% of executives said that their institution doesn't use any software for AML transaction monitoring. This approach is unlikely to remain feasible as firms face requirements to monitor larger volumes of transactions.

Asset management institutions often have different technology needs, however, since many rely on the IT systems of third-party transfer agencies. Although 33% of asset management executives said that their institution doesn't use software for AML transaction monitoring, most transfer agencies have embedded IT systems that have been designed to identify suspicious activity.

Institutions use a wide variety of different AML applications, with no one vendor application having a dominant position. (See Exhibit 6.) In OFAC screening applications, the leading vendors were Thomson Financial, named by 32% of the executives' institutions, and Bridger Systems, by 26%. Yet 40% of executives cited an assortment of other applications.

Use of vendor applications in AML transaction monitoring is even more diverse. (See Exhibit 6.) The most popular vendors were Prime Associates and ATCHLEY, cited by only 14% and 11% of executives, respectively. Fully 61% of executives cited a variety of other vendors, with each named by less than 3% of executives.

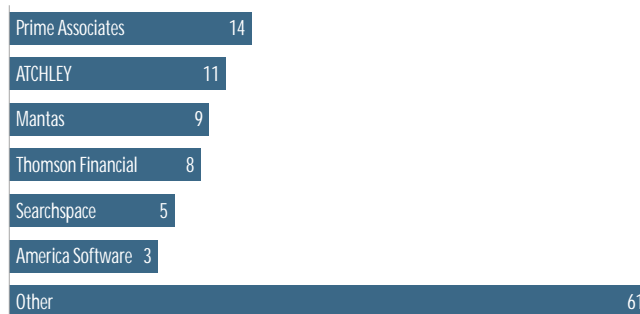
Exhibit 6 | Vendor Applications Used

Percent of Executives Reporting Firm Uses Each Application in OFAC Screening
Base = Firms That Use Vendor Applications for OFAC screening



Percent of Executives Reporting Firm Uses Each Application
In AML Transaction Monitoring

Base = Firms That Use Vendor Applications in AML Transaction Monitoring



The most important factors in selecting a vendor application for OFAC screening or AML transaction monitoring were the effectiveness of screening and the functionality of the application with more than 90% of executives rating these factors as very or extremely important. (See Exhibit 7.) Also ranked highly were vendor capability and reputation and the ease of installing and learning the application, each rated as very or extremely important by roughly 80% or more of executives for selecting both types of applications.

Although cost is an important factor, rated as very or extremely important by roughly three-quarters of executives for both types of applications, cost considerations clearly take a back seat to other factors, in particular functionality and screening effectiveness.

Exhibit 7 | Importance of Factors in Choice of Vendor Applications

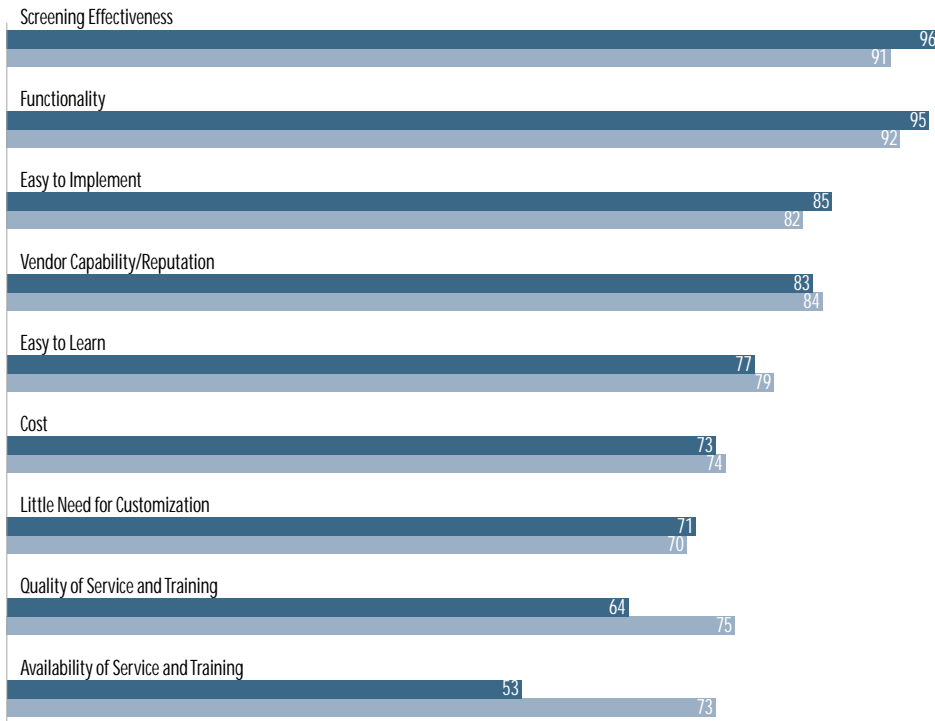
Percent of Executives Rating Factor as Very or Extremely Important

Base = Firms That Use Vendor Applications for OFAC Screening or AML

Transaction Monitoring

■ = OFAC Screening

■ = AML Transaction Monitoring



Methodology

Deloitte & Touche surveyed 167 senior financial services executives with AML responsibilities through an Internet questionnaire on June 18 to 24, 2003. The executives surveyed worked at institutions with a variety of sizes—20% at institutions with less than \$1 billion in assets, 47% at institutions with \$1 billion to less than \$100 billion in assets, and 33% at institutions with \$100 billion or more in assets. Executives had AML responsibilities in a variety of types of financial services—63% in securities, 32% in banking, 31% in asset management, 26% in insurance, and 13% in transfer agency. (The total is greater than 100% since some executives had AML responsibilities in more than one type of financial service.) Bayer Consulting conducted the survey and assisted with the analysis of the survey data.

About Deloitte & Touche

Deloitte Touche Tohmatsu is one of the world's leading professional services organizations, delivering world-class assurance and advisory, tax, and consulting services through its national practices. More than 120,000 people in 150 countries serve over one-quarter of the world's largest companies, as well as large national enterprises, public institutions, and successful, fast-growing global growth companies.

Our internationally experienced professionals strive to deliver seamless, consistent services wherever our clients operate. Our mission is to help our clients and our people excel.

Deloitte Touche Tohmatsu serves financial services firms globally through our Global Financial Services Industry practice. GFSI's industry specialists represent every major financial center in the world and bring decades of experience and leadership in banking, securities, insurance, and investment management to each client assignment.

For more information about our practice, visit our website at www.dttgfsi.com/aml.

© 2003 Deloitte & Touche LLP.
Deloitte & Touche refers to Deloitte & Touche LLP and related entities.
All rights reserved.

0903 - #3171

**Deloitte
Touche
Tohmatsu**