Navigating the PEP Landscape:
Part II: Assessing the Risks

Identify and manage PEP exposure with tools to pinpoint risk before it impacts profit.

October 2009

Research provided by:
Kristine Regele, CAMS
Senior Compliance Analyst
LexisNexis®
Assessing the risks
Assessing the risks of doing business with a Politically Exposed Person (PEP) is no easy task.

As we discussed in Part I of our PEP series, financial institutions that maintain business relationships with PEPs face greater risks because of the heightened possibility that such individuals could misuse their power and influence for personal gain. However, because many PEPs do not abuse their positions, the risks of doing business with a PEP cannot be determined by this classification alone.

Assessing the risks of doing business with a PEP boils down to evaluating the individual’s risk for money laundering. In the same way that private banking is considered to be a higher-risk product regardless of the customers who choose it, PEPs generally pose elevated risks to financial institutions regardless of the product they choose. According to the Federal Financial Institutions Examination Council’s (FFIEC) Bank Secrecy Act/Anti-Money Laundering Examination Manual, “banks should take all reasonable steps to ensure that they do not knowingly or unwittingly assist in hiding or moving the proceeds of corruption by senior foreign political figures and their associates. Because the risks presented by PEPs will vary, controls and monitoring related to these accounts and transactions should be risk-based.”

Section 352 of the USA PATRIOT Act requires financial institutions to establish anti-money laundering programs and prescribes minimum components to help ensure the effectiveness of those programs. Regulatory expectations include designing an Anti-Money Laundering (AML) program that is commensurate with the risks identified in a risk analysis. For an institution to effectively mitigate overall money laundering risk, it should evaluate both customers and transactions using a risk-based approach. The risk-based AML program will involve a combination of systems and policies designed to tackle different types and levels of risk, including screening for economic sanctions and identifying PEPs. Therein lies the challenge.

There are dozens of government sanctions lists available throughout the world—including those from the United Nations, the U.S. Office of Foreign Assets Control (OFAC) and Canada’s Office of the Superintendent of Financial Institutions (OSFI)—that ban or restrict financial institutions from conducting business with specific individuals, entities and countries. Screening customers against published lists is relatively simple. However, determining whether an individual is a PEP and then determining the risk of doing business with that PEP is far more onerous a challenge in part because there is no universal PEP list.
The Wolsfberg Group recommends that individual countries identify and publish lists of PEPs—including their close associates and family members—within their own borders to help ease the burden on financial institutions. However, to date, only Uruguay has published such a list.

As such, to ensure their compliance, financial institutions typically employ a multi-dimensional approach to assessing the presence of PEPs. There are many recommendations for executing such an approach.

**Risk-assessment guidelines**

In addition to basic due diligence measures, the Financial Action Task Force’s 40 Recommendations on Money Laundering states that financial institutions should, in relation to politically exposed persons both foreign and domestic:

- Have appropriate risk-management systems to determine whether the customer is a politically exposed person.
- Obtain senior management approval for establishing business relationships with such customers.
- Take reasonable measures to establish the source of wealth and source of funds.
- Conduct enhanced ongoing monitoring of the business relationship.

According to the Wolfsberg Group, a wide range of controls may be considered for the identification and management of PEP relationships, but not all will be appropriate for application across an institution’s entire range of business. For example, in retail banking relationships, a different balance of controls may be relevant than those considered appropriate within a private banking/wealth management environment:

- **New client approval**: Institutions should have reasonable procedures designed to identify PEPs either before the relationship is established or shortly thereafter, where permitted under applicable law. While basic client relationships are typically subject to standard due diligence during the approval process, PEP relationships should be escalated for approval by senior management.

- **Identification existing clients**: When an institution becomes aware that an existing client has become a PEP, it should apply appropriate enhanced procedures and controls and notify senior management.

- **Enhanced due diligence**: Once identified and depending on the product or service sought, additional research and analysis may be appropriate including validation of information provided for a number of factors including an understanding of the individual’s source of funds and wealth.

- **Enhanced monitoring**: Accounts with a PEP relationship should be subject to enhanced monitoring to detect unusual and potentially suspicious activity.

- **Review existing PEP clients**: Such relationships should be subject to periodic review to ensure that due diligence information remains current and the risk assessment and associated controls remain appropriate. Senior management should approve these reviews.

- **Training and education**: A financial institution’s staff members are the first line of defense in preventing and detecting money laundering, and they play a crucial role in identifying clients or potential clients who are PEPs. It is therefore vital that the risks, policies, procedures and processes associated with such individuals are communicated to relevant employees and form part of the institution’s regular AML training program.
At a minimum, the FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual states that due diligence procedures should include, but should not be limited to, the following:

- Identify the account holder and beneficial owner.
- Seek information directly from the individual regarding possible PEP status.
- Identify the account holder’s country of residence.
- Obtain information regarding employment or other sources of funds.
- Check references, as appropriate, to determine whether the individual is or has been a PEP.
- Identify the source of wealth.
- Obtain information about immediate family members or close associates who have transaction authority over the account.
- Determine the purpose of the account and the expected volume and nature of account activity.
- Make reasonable efforts to review public sources of information. These sources will vary depending upon each situation; however, banks should check the account holder against reasonably accessible public databases (e.g., government databases, major news publications, free commercial databases available on the Internet and fee-based databases, as appropriate).

**AML risk-assessment solutions**

Automated screening tools have revolutionized the manner in which financial institutions screen and monitor their customers and transactions. Businesses can choose from a plethora of screening options, from online applications to batch processing, allowing customers to decide what is most important to them—immediate access to high-volume processing or fully automated and immediate results.

While many of these solutions are quick and easy to use, not all are designed to reduce your employees’ workloads by streamlining and supporting compliance processes. Integrating screening solutions into your customer on-boarding tool eliminates the need to manually enter data twice. Batch screening can help compliance professionals easily check and re-screen thousands of customers at a time using any number of data filters. Robust algorithms with organization-specific configurability can help you reduce occurrences of potential matches that require manual reviews. When you need to analyze an exception, integrating enhanced due diligence and research tools can save your compliance analysts significant time. Obviously, these are designed to detect risk and filter it before your institution ever becomes involved in money laundering.
But the effective AML program doesn’t stop there. Continuous customer monitoring with resulting risk alerts can help detect changes in risk profiles and identify potentially suspicious activity and report it as required by law.

An effective screening program would include:

- **A subscription to a commercial PEP database**: There are multiple PEP-screening databases on the market that include information about hundreds of thousands of high-risk and sanctioned individuals and entities and their networks culled from public records and global media. Such a database is critical to any effective screening program.

- **Name-matching software**: These software systems, available from a variety of vendors, are designed to produce matches between individuals and entities listed in commercial databases or watch lists and names of individuals and entities generated by the institution. Most organizations scan existing customers, potential customers and their associates. While matching software significantly speeds up the name-comparison process, further investigation is typically required to determine whether it is a false positive or a true match. This has been a challenge for many organizations. The true cost of a software solution therefore includes not only the product price tag, but also the cost of human resources needed to disposition the alerts. We will discuss this in greater detail in Part III of our series.

- **People**: The items listed above are merely tools to help you get to know your customer and evaluate the risks present to your financial institution. They are intended to complement, not to be a substitute for, the most valuable asset of any compliance regime—its personnel.

### Choosing a solution

It is important to understand that not all tools are created equal. It is the institution’s responsibility to check the quality of the tools they use and the expertise of the developers. Compliance professionals shopping for technological solutions to PEP screening should consider:

- **Who is the vendor?** Make sure to choose products from a vendor you trust, rather than a fly-by-night operation. The bottom line is that it is the financial institution that is responsible for compliance, not the developer.

- **What is the scope of the product?** Does the database merely contain information about PEPs, their families and their associates, or does it also include other high-risk individuals or those named on government watch lists? How sophisticated is the matching software? It is important to remember that financial institutions must evaluate both PEPs and other high-risk customers to satisfy regulators.

- **What is the methodology?** How does the vendor compile the database? What sources does the database use? Are the sources reputable? How does the software filter matches? How often is the product updated?

It’s also important to remember that technology is only as good as the information we supply it with. These are merely tools, and even the most sophisticated technology can require additional analysis.

In Part III of our PEP series, we will show you how to overcome some of the challenges of the risk-assessment process.
Sources


For more information:
Call 866.858.7246 or visit lexisnexis.com/risk/financial-services

About LexisNexis® Risk Solutions
LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

Our financial services solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.