



YOU CAN'T TELL THE PLAYERS WITHOUT A PROGRAM – Customer risk assessment for Bank Secrecy Act and Anti-Money Laundering compliance.

Even though financial institutions were required to implement Anti-Money Laundering (AML) compliance programs by 1 October, 2003, many financial institutions are still struggling with the intricacies involved. NCUA has not yet reached the same level of enforcement practiced by other financial regulators, so there is time to further improve AML programs.

One of the key elements of AML compliance is the *customer risk assessment*. The Bank Secrecy Act (BSA) calls for a Customer Identification Program (CIP) that includes a “*risk-based assessment of customer risk*.”

In June 2005, the Federal Financial Institutions Examination Council (FFIEC) published the “Bank Secrecy Act/Anti-Money Laundering Examination Manual”.¹ While the document does not contain all the information you may need, if you use it as a guide you can't go far wrong.

The CIP focuses on identifying potential customer risk at two levels. The first is at the level of the credit union itself. This assessment should include risks related to the:

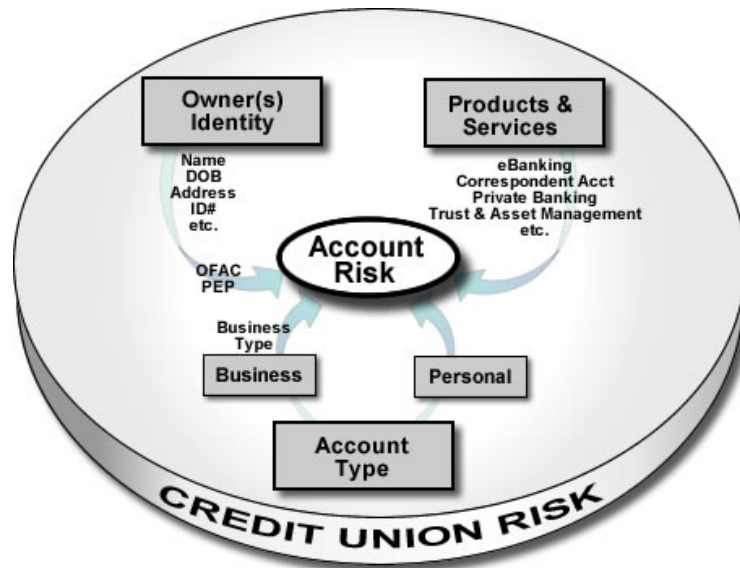
- √ **Types of accounts offered.** Money laundering introduces illicitly derived funds into the financial system, structuring those funds and distributing them through domestic and international banking systems. Products and services that facilitate this process should be considered higher risk.
- √ **Methods of opening accounts.** Accounts opened in person may offer less risk than accounts opened remotely (e.g., Internet).
- √ **Types of identifying information available.** The completeness of the information collected and its infusion in the organization's data process supports AML risk assessment and management.
- √ **Credit union size, location, and customer base.** The organization's size (e.g., more members, more risk), location(s) (e.g., urban versus rural, High Intensity Financial Crime Area), and customer base (e.g., education level, profession, income, etc.) proscribe important parts of its vulnerability.

¹ Federal Financial Institutions Examination Council, BSA/AML Examination Manual :
http://www.ffeec.gov/bsa_aml_infobase/pages_manual/manual_online.htm
http://www.ffeec.gov/bsa_aml_infobase/documents/BSA_AML_Man.pdf

Each of these factors should be included in the self assessment of AML/CIP risk for the organization. The individual risk factors should be prioritized (e.g., low, moderate, high – as shown in Appendix J of the FFIEC AML Examiner’s Manual) and documented as part of the AML program.

The second level of assessment is to determine the potential risk of the individual member, which is a bit more complex.

There are at least three categories of information that will bear on the risk associated with any particular new account: the owner(s) identity, the products and services involved and the account type.



Owner’s identity – The regulation requires that, as a minimum, the name, date of birth, address and identity number (e.g., SSN, DLN) be collected and retained. The identity information must be verified to provide reasonable confidence that the true identity of the member is known. There may be components of the member’s identity that will require further due diligence. Among these may be: resident or non-resident aliens, embassy and foreign consulate accounts, and corporate accounts owned by International Business Companies (IBC) or Private Investment Companies (PIC). All new members must be searched against the Office of Foreign Assets Control (OFAC) file to determine if they may be a denied party. An additional search must be made to determine if the individual, his family or associates may be Politically Exposed Persons (PEP). This is one of the more complex issues, but there are various ways to perform this search and there are commercial international databases available.

Products and services involved – The regulations outline those products and services that are considered to be higher risk for money laundering. These include, but are not limited to:

- √ Correspondent banking
- √ Electronic payment services

- √ Lending activities
- √ Trade finance activities
- √ Private banking
- √ Trust and Asset Management Services
- √ Purchase and conversion of monetary instruments

Most financial services carry some degree of money laundering risk, but it is important that these risks be assessed in the context of the overall credit union vulnerabilities.

Account type – Personal accounts must be monitored carefully, but business accounts carry with them another dimension of risk depending on the type of business involved. The instructions on Treasury Form TD F 90-22.53, Designation of Exempt Person ², list exemption ineligible businesses that can be used as a starting point for identifying high risk. These include, for example, businesses:

- √ Serving as financial institutions or agents of financial institutions of any type;
- √ Engaged in purchase or sale to customers of motor vehicles of any kind, vessels, aircraft, farm equipment or mobile homes;
- √ Practicing law, accountancy, or medicine;
- √ Chartering or operation of ships, buses, or aircraft;
- √ Involved in gaming of any kind (other than licensed pari-mutuel betting at race tracks);
Performing investment advisory services or investment banking services;
- √ Engaged in real estate brokerage, pawn brokerage, title insurance and real estate closing, or trade union activities.

There are many other types of businesses that exhibit risk, such as: parking lots, video rental stores, fast food restaurants and pizza parlors, and money services business (MSBs). The U.S. Census Bureau's database for the North American Industrial Classification System (NAICS) provides a good reference for formally defined business types.³ It is important your program identify business types and assess their risk.

You should remember that the Financial Crimes Enforcement Network (FINCEN) has authority to add to lists of entities considered high risk. Frequent visits to the FINCEN web site are highly advisable.⁴

We can't cover all of the details of customer risk assessment in a short article. The elements described above are a start. Once you have created the mechanism to detect each of the risk categories that

² http://www.ncua.gov/reg_alerts/Prior2003/99-RA-1.pdf

³ <http://www.census.gov/epcd/naics02/naicod02.htm>

⁴ <http://www.fincen.gov/>

impact your overall risk, you should then create a process for prioritizing each account's risk. Risk identified during account opening should be carried along to the account activity monitoring process so that it is considered during the identification of suspicious activities.

Implementing a comprehensive CIP is not easy and is a work that is still in progress at most financial institutions. Fully understanding the risks related to money laundering and terrorism financing may take years. Efforts to create a viable program are usually recognized by examiners. Not making an effort may draw a much different reaction.

Bob Cofod is the President and founder of BANKDetect, which provides loss prevention and anti-money laundering compliance services to financial institutions. He has over thirty-five years experience developing and operating advanced analytical systems for the U.S. military/intelligence, healthcare and financial communities. He has been a speaker and author in various banking venues on the topic of loss prevention and anti-money laundering analysis. He may be reached at bob.cofod@bankdetect.com.