

METAVANTE WHITE PAPER

Customer Risk Assessment

Christopher Price
Metavante Compliance Consultant

 **Metavante**[®]
Risk and Compliance Solutions

Introduction

In the past four years, much attention has been focused on Section 352 of the USA PATRIOT Act – the ability to monitor client activity to detect suspicious activity. Anti-money laundering (AML) monitoring technologies have proliferated throughout the world-wide compliance landscape, and any financial institution (FI) that is in need of AML detection technology can speak to many vendors in that arena.

More recently, a growing area of focus, especially in the United States, is on Section 326, which outlines Know Your Customer (KYC) and Customer Identification Program (CIP) requirements for an FI. These represent some of the most basic tenets of the USA PATRIOT Act, because of their importance to a sound compliance program.

With the focus shifting to CIP/KYC, FIs are rethinking their client relationships and their client acceptance process. Firms that have given this problem the attention it deserves typically attack the problem from multiple angles. The first area is risk assessment. How do you actually risk-assess your existing client base and any new prospective clients? For most FIs this is an area that was never fully addressed and presents tremendous challenges. No longer can you simply establish risk categories that have little or no quantitative merit. Risk assessment is a science that requires real analytics and significant processes behind it.

Secondly, the process known as customer acceptance, or the ability to determine based on client type what the firm expects to know about any new prospect, is a key factor in KYC programs. Because there may exist a multitude of client types, especially in FIs that offer a rich set of products and services, customer acceptance processes must be segmented and detailed for each client type.

The issue of customer identity, or truly knowing the customer, is the basic foundation on which Section 326 is built. Identity verification techniques and customer assessments against criminal, global sanctions, and politically exposed person (PEP) databases are linchpins in this requirement. This white paper is intended to give the reader an overview of the customer risk assessment process, and it includes examples and an illustration.

BSA/AML Risk Assessment Role in Validating the Customer Risk Assessment

Banks and other FIs are encouraged by the federal functional regulators to conduct annual risk assessments of the institutional exposure to potential money laundering and terrorist financing. For a look at the regulatory requirements surrounding a BSA/AML Risk Assessment, please select the following link:

http://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_005.htm

The BSA/AML Risk Assessment serves as the road map for guiding the AML Risk Management team in the implementation of procedures and internal controls for comprehensive KYC/CIP, recordkeeping, and suspicious activity monitoring and reporting. The BSA/AML Risk Assessment considers the following:

1. Geography – including the FI's jurisdiction, branches, the geographic regions of the customer base, and the jurisdiction of counterparties
2. Customers – defining customer types, with particular concern for the identification of customer/entity types conventionally associated with a heightened risk for money laundering/terrorist financing exposure, such as cash-intensive businesses, import/export companies, and PEPs
3. Products and services offered by the institution – certain products and services pose a greater risk of money laundering and terrorist financing, such as private banking, international wire transfers, and trade finance

The BSA/AML Risk Assessment allows the institution to define customer types to varying degrees of granularity. For example, customer types may be defined simply as individuals and businesses. More granular definitions may include individuals, corporations, professional service providers (PSP), non-government organizations (NGO), government organizations, cash-intensive businesses, non-bank financial institutions (NBFI), etc.

Having defined and identified customer types and the various geographies that the institution services respectively, customer acceptance criteria can be established. This will include basic customer due diligence, documentary and non-documentary identification, and for customers conventionally associated in the industry as having heightened exposure to potential money laundering risk, enhanced due diligence.

Know Your Customer and Customer Acceptance Criteria

Availability of KYC Data

The BSA/AML Risk Assessment, in identifying areas of exposure, allows AML Risk Management to define the customer acceptance criteria that will form the basis for the KYC program. It is of no small concern that the KYC data that is subsequently collected and fed into the core banking system be readily available for use in the AML software in which risk modeling is conducted. An institution's AML program may have a very rigorous and robust KYC program, complete with stringent account opening procedures; however, if this data is not readily available, then FIs face the prospect of limited risk factors for consideration in their risk modeling.

Initial Risk Rating at Account Opening Stage

Before the actual risk rating process takes place, some FIs may apply an initial risk rating to customers, depending upon the policy of the institution. For example, if the risk rating process requires the tabulation of historical transaction activity, this factor will not be available for a new customer. There are various options available to the FI in such a case. One option is the application of a *default* risk rating, which automatically flags the new customer for a probationary period wherein the customer is subjected to closer scrutiny until a risk rating is applied under the FI's risk model. Another option requires the collection of expected or anticipated transaction volumes/amounts as part of the KYC at account opening. Again, if/when this information is fed to the AML software solution; it can be used in applying an initial risk rating as well as in determining the customer profile. For certain customer types, the FI can consider the average transaction volumes for customers of the same and similar customer types, and use that initially until the new customer has enough transaction history.

If the customer is of a type conventionally associated with heightened risk of money laundering exposure, then the FI may apply a high risk rating initially as a default for specified customer types. These customer types would probably be subject to Enhanced Due Diligence (EDD), and they may include cash-intensive businesses, shell corporations, NBFIs, import/export companies, foreign banks, offshore entities, etc.

A customer may be assigned a *high* or *very high* risk rating, regardless of any other risk factor, if it is determined that a *dominant* risk factor applies to that particular customer. A dominant risk factor is an item determined by the FI to weigh so heavily in terms of potential risk exposure, that customers to whom/which it applies are automatically placed in a high or very high risk category. An example of such a risk factor is PEP status. In this example, the FI accepts a new customer, either individual or other customer type, which is identified either through the account opening questionnaire, a PEP database screening, or other public search database as having a PEP status. If the FI has deemed PEP status as a dominant risk factor, then regardless of the other risk factors that would have been considered in the risk rating process, this new customer would receive a high or very high risk rating.

Risk Modeling

Risk Factor Categories

Risk factors can be internal, external, or calculated. The availability and form of data that AML Risk Management can use, determines which category the risk factor falls into.

Risk factors that are readily available in the AML software solution are referred to as *internal* risk factors. Because internal risk factors are readily available in the AML software solution, these are the easiest and most expedient to use. Presuming this data is readily fed to the AML software solution, examples may include country of incorporation, country of residency, NAICS Code or SIC (if the model is not itself based upon an NAICS Code or SIC), and *HIFCA* and/or *HIDTA* U.S. geographical designation.

Risk factors that require a formula calculation based upon available data are referred to as *calculated* risk factors. Examples include average or total cash volume over a specific period, average or total wire volume over a specified period, and total activity volume over a specified period.

Risk factors that must be input manually are referred to as *external* risk factors. Depending upon the size of the FI, this may be relatively simple or very tedious and time consuming. Common examples include the existence of negative press, subpoenas, and SAR filings. FIs with a very small customer base may find the input of external risk factors to be plausible, but medium to large FIs usually abstain from using them in the risk models.

As previously mentioned, an FI may also designate certain risk factors as dominant. Since there may be existing customers that are discovered to have a dominant risk factor that was not previously identified at the time of the establishment of the customer relationship, or was not required for KYC consideration at the time, this dominant risk item may be applied to a customer with an existing risk classification of other than *high* or *very high*, and result in an elevation of the risk classification. In certain circumstances, a particular risk model may have more than one dominant risk factor that does not apply to other risk models. For example, an FI may determine that both PEP status and foreign country residency for a PSP are dominant risk factors, whereas risk models for other customer types may only consider PEP status; it is a risk management decision. Depending upon the AML software solution, this may require specialized programming.

The following factors should be considered in building customer risk models:

CUSTOMER TYPES

The building of customer risk models is highly dependent upon decisions made when defining customer types. Some organizations may simply define and distinguish customer types as individual and business. Other organizations may require more specific definitions. For example, international individual, domestic individual, broker dealer, partnership, international corporation, domestic corporation, trust, correspondent bank, foreign banking institution, money service business, cash-intensive business, NBFIs, etc.

The first step in building the customer risk models involves listing customer types at the lowest level possible, defining the CIP acceptance criteria and the customer risk factors for each type. Once these steps are completed, you can merge those that share the exact same components. Keep in mind that multiple customer types can be linked to one model.

A fairly expedient method of applying different customers to the correct model is to assign based upon the NAICS Code, in the case of non-individuals.

It is important to note that customer types that you define should also be defined in the source system that will supply the customer file.

ACCOUNT TYPES

Account types should be factored into the calculation of customer risk by applying a risk factor such as an evaluation of the type of account(s) and account activity volume. For example, a corporate DDA compared to a certificate of deposit for a domestic individual would result in differing risk result scores. Similarly, an IRA for a professional service provider would carry a different risk result score from a transaction account, such as a business checking account. A private banking account carries a significantly different result score from a corporate CD.

ACTIVITY TYPES

Type of activity should be factored into the calculation of customer risk by applying a risk factor such as an evaluation of the products or services utilized or customer/account activity volume. For example, international wire transfers receive a higher risk than check deposits. In another example, payable upon proper ID (PUPID) wires would carry a higher risk than automatic bi-weekly ACH payroll deposits.

OTHER FACTORS

FIs can utilize other factors with varying weights and result scores. For example:

- Type of business (if the model is not first based upon the NAICS or SIC for entities)
- Occupation (for individuals)
- Length of relationship
- Relationship history, i.e., *CTR customer, subject of SAR filing, subject of subpoena, subject of negative press*
- Cash activity volume
- Wire activity volume
- Total volume
- Country of residency
- Country of incorporation

RELATIVE RISK WEIGHTS AND RESULT SCORE CONTRIBUTIONS

The weight of each risk factor applied is a subjective risk management decision that is determined relative to other risk factors. For example, the relative weight of average cash volume for an NBF title company may be greater than the weight applied to average wire volume, since title companies are expected to engage in extensive wire activity, but only small-volume cash activity. In another example, the country of incorporation for a corporation may carry a certain weight, but AML Risk Management may deem that relationship history (CTR filings, negative press, subpoenas, and SAR filings) carries a greater relative weight. Obviously, such a factor would be more significant for existing customers than for new customers. The relative risk weights should add up to 100 percent.

The result score contribution is the value applied to a possible risk factor result. For example, if country of incorporation is a risk factor, the following table illustrates possible result score contributions:

Country of Incorporation

U.S.	25
Foreign – FATF Member	50
Foreign – NCCT, INCSR, Corruptions Perception Index, other citation for weak AML regimes	75
Foreign – OFAC , Offshore Tax Haven, Section 311, etc.	100

The result score contribution is multiplied against the relative risk weight, to arrive at a risk factor score. This is added to other risk factor scores to arrive at a total risk score. Examples of risk models for NBFIs and for PSPs respectively are illustrated on the following pages. Note that NAICS Codes determine which model a customer is apportioned to in these two sample risk models.

Non-Bank Financial Institution*				
Risk Factor	Relative Risk Factor Weight	Possible Results	Result Score Contribution	Evaluation of Customer X
Country of Inc.	20%	Result 1 – United States Non-HIFCA/HIDTA	25	
	20%	Result 2 – FATF Members/Nations Other than Results 3 and 4	50	
	20%	Result 3 – Nations Formerly on NCCT List within Past 3 Years	75	
	20%	Result 4 – Nations Sponsoring Terror, Drug Trafficking, and Weak AML Regimes; Offshore Tax Havens	100	
Cash Activity Volume	40%	Result 1 (1– X)	25	
	40%	Result 2 (X – XXX)	50	
	40%	Result 3 (XXX-XXXX)	75	
	40%	Result 4 (XXXX-XXXXX)	100	
		Default (No Activity)		
Wire Activity Volume	40%	Result 1 (1– X)	25	
	40%	Result 2 (X – XXX)	50	
	40%	Result 3 (XXX-XXXX)	75	
	40%	Result 4 (XXXX-XXXXX)	100	
		Default (No Activity)		
PEP (Signer) – Dominant Risk Item	Automatic High Risk	Result 1 – Yes	Automatic High Risk	
	0%	Result 2 – No	0	
Total Risk Score	100%			
				Results =
				Score Range
			Very High Risk	76 - 100
			High Risk	51 - 75
	Sample risk score attribution		Medium Risk	26 - 50
			Low Risk	0 - 25

*NAICS Codes Covering Casinos, Card Clubs, MSBs, Precious Metals/Stones Dealers, Pawn Brokers, Loan or Finance Companies, Foreign Exchange Houses, Futures Commissions Merchants, Insurance Companies, Real Estate Brokers, Notaries, and Investment Brokers

Professional Service Providers**					
Risk Factor	Relative Risk Factor Weight	Possible Results	Result Score Contribution		Evaluation of Customer X
Country of Domicile	10%	Result 1 – United States Non-HIFCA/HIDTA	25		
	10%	Result 2 – FATF Members/Nations Other than Results 3 and 4	50		
	10%	Result 3 – Nations Formerly on NCCT List within Past 3 Years	75		
	10%	Result 4 – Nations Sponsoring Terror, Drug Trafficking, and Weak AML Regimes; Offshore Tax Havens, U.S. HIFCA/HIDTA	100		
Cash Activity Volume	40%	Result 1 (1– X)	25		
	40%	Result 2 (X – XXX)	50		
	40%	Result 3 (XXX-XXXX)	75		
	40%	Result 4 (XXXX-XXXXX)	100		
		Default (No Activity)			
Wire Activity Volume	40%	Result 1 (1– X)	25		
	40%	Result 2 (X – XXX)	50		
	40%	Result 3 (XXX-XXXX)	75		
	40%	Result 4 (XXXX-XXXXX)	100		
		Default (No Activity)			
Length of Relationship	10%	Result 1 (>5 years)	25		
	10%	Result 2 (3 - 5 years)	50		
	10%	Result 3 (1 - 3 years)	75		
	10%	Result 4 (0 - 11 months)	100		
PEP (Signer) – Dominant Risk Item	Automatic High Risk	Result 1 – Yes	Automatic High Risk		
	0%	Result 2 – No	0		
Total Risk Score					
					Result =
					Score Range
			Very High Risk		76 - 100
			High Risk		51 - 75
	Sample risk score attribution		Medium Risk		26 - 50
			Low Risk		0 - 25

**NAICS Codes Covering Lawyers, Accountants, Financial Consultants, and Other Gatekeeper Occupations

Risk Classifications

Customers should be categorized into risk-assessed groups titled *risk classes*. Risk classes may be simple in development, such as low, medium, and high, or they can be more elaborate, such as low, medium, medium-high, high, and very high. Smaller institutions with simpler business profiles can apply a simple risk classification schematic, whereas more complex institutions may opt for a more expansive risk classification schematic. For domestic institutions with a U.S.-based Board of Directors, the risk classification schematic that AML Risk Management develops should be presented to the Board for approval -- for U.S. branches and agencies of foreign banks, the highest managerial authority in the U.S.

Each risk class should carry a numeric range into which a customer will fall based upon that customer's score through risk modeling. Each risk classification, in turn, will have an applied tolerance.

Customer Profiles

Once a customer has been assigned a risk class, a tolerance is applied to the expected incoming and outgoing volumes for profile-monitoring purposes. The tolerance is inversely related to the risk class; thus, the higher the risk, the lower the tolerance. Note the following example:

Low Risk – 80% tolerance

Medium Risk – 50% tolerance

High Risk – 20% tolerance

Thus, if customer ABC Importers, a medium risk customer, has an expected monthly dollar volume of \$50,000 incoming and \$40,000 outgoing, then profile-based monitoring would result in a flag only if the following thresholds were exceeded:

Incoming = \$75,000 = Expected incoming of \$50,000 x 50% tolerance = \$25,000 + \$50,000

Outgoing = \$60,000 = Expected outgoing of \$40,000 x 50% tolerance = \$20,000 + \$40,000

The same would be applied if the numbers of incoming and outgoing transactions are considered.

Sample Risk Assessment Scenario – XYZ Bank

XYZ Bank is a port-city bank that is foreign-owned. It serves customers situated throughout the state of Florida, and the Commonwealth of Puerto Rico, as well as Central and South America. XYZ provides both traditional retail banking services as well as wholesale banking services to corporations, small businesses, a small population of charities and NGO customers, and two foreign banks located in South America.

XYZ completed its annual BSA/AML Risk Assessment and was able to define multiple customer types. AML Risk Management decided that the existing customer risk models, which were designed for individuals and businesses, were not adequate, and has designed more granular risk models to reflect the various customer types it has defined.

CUSTOMER TYPES DEFINED

Domestic Individuals	Foreign Banks
Non-Resident Aliens	Embassy/Consulates
U.S. Corporations	Non-Bank Financial Institutions
Foreign Corporations	Non-Government Organizations
Professional Service Providers	

XYZ has only two foreign bank correspondent relationships and knows that foreign correspondent accounts are always subject to intense scrutiny by the federal functional regulators. AML Risk Management decides not to apply the foreign banks to any risk model, but manually inputs them as high risk and subjects the accounts to both profile-based monitoring and periodic account reviews.

XYZ next has to determine if it will segregate similar customer types into separate risk models based upon domestic or foreign designation. The implication of doing so would result in a greater number of risk models, and it may create additional workflow steps. After careful consideration, customers with the same NAICS Code will not be segregated into separate risk models by geographic jurisdiction, but rather, one risk model for the same customer types will consider geographical risk factors. Thus, one individual risk model will cover both domestic individuals and foreign individuals; one risk model for PSPs will cover both domestic and foreign PSPs, etc.

XYZ has determined that the following KYC data is available from the core system for use in the new risk models:

- NAICS Code
- Country of Incorporation
- Country of Residency
- Length of Relationship
- Account Type
- Occupation

These represent internal risk factors for XYZ to consider. Due to the size of the customer base, the use of external risk factors, such as SAR filings, country of suppliers/counterparties, etc., is not plausible.

XYZ is concerned that certain customers that are associated with heightened risk for AML exposure in the industry may in fact have other mitigating factors that would actually place them in a low- to medium- risk class. For example, some MSB customers may have low cash and/or wire volume relative to other high-risk MSBs. XYZ decides that it will utilize average cash volume and average wire volume for a six-month period as risk factors. Acquiring these factors will require a query of existing data and a mathematical formula. Thus these are calculated risk factors.

Finally, XYZ determines that a particular risk factor, if present, will automatically result in a high-risk classification, regardless of the other risk factors. Any customer with a PEP designation will automatically carry a high-risk classification. Based upon AML Risk Management's past experience with PSP customers, it also decides to add a special second dominant risk item to its risk model for PSPs. While country of residency is already a risk factor in each of the models, if a PSP customer is foreign-based, this will automatically result in a high-risk classification. This too may require specialized programming of the AML software.

XYZ has decided upon a simple risk classification schematic of low, medium, and high:

Risk Class	Lower Bound	Upper Bound
Low	0	40
Medium	41	80
High	81	100

XYZ has created the skeleton of its risk models by determining that NAICS Codes will allocate customers to a particular risk model, determining which factors are available from the KYC data, and establishing the risk classes. Now, specific risk factors must be applied to specific models, with relative risk weights and result score contributions. Generally, the result score contributions should be the same across models for the same factor, but the relative risk weights may differ.

Regulators and Technology

The ability to collect and electronically store relevant data on a client so that it is both easily accessible to compliance professionals and regulators is yet another challenge to be met.

Thus, sound CIP/KYC processes must utilize systems of record, with client data stored and/or imaged for instant access. This means a central data warehouse of not only basic client data, but also of all methodologies that are specific to identify verification (IDV), CIP, and KYC metrics.

Regulators have stepped up their focus and approach to these CIP/KYC issues and are demanding a well-thought-out process that is logical, analytic, and defensible. Gone are the days of simply performing mass categorizations of clients. Regulators want you to clearly demonstrate your risk modeling and the rationale of how you developed it. All of this will help show them that you understand your clients and the perceived risks associated with the different segments of your base.

While regulators are quick to indicate that technology need not be the only mechanism that can solve these requirements, technology does allow for the honing of algorithms, the electronic recording of client data, the ability to scan critical compliance databases, electronic IDV validation, and the ability to store all client data centrally.

Metavante Risk and Compliance Consulting

Metavante Risk and Compliance Solutions assist financial institutions in developing efficient and sustainable risk programs. With compliance consulting from Metavante Risk and Compliance Solutions, financial institutions gain the expertise to help them evaluate the strengths and weaknesses of their AML efforts, define enterprise-wide and customer-level risk models, and gain a solid business perspective during the implementation of AML software solutions.

To learn more, call **1-877-487-6330** or visit us at metavanteriskandcompliance.com.