AML Risk Assessment: Laying the Foundation

By Laura H. Goldzung, CFE, CAMS, CFCS

Reasonably designed. Risk-based. Mitigating Controls. Adopted and Approved. Fully Implemented. Effectively Managed. Inherent and Residual. Appropriate.

We all know these terms and hear them day-in and day-out in the world of AML. But how many of us truly understand how they relate to risk? When I first came to the land of AML following the events 9-11, I asked myself, "How do we know what the risks are without taking a careful inventory of who we are, what we offer, where and to whom we offer it, and how we deliver it?" Seems simple enough on the face of it.

Every day, as individuals and consumers, we encounter many ways in which we navigate risk and make decisions, and some of our decisions pose higher risk than others.

Remember when you were applying for that pre-approved mortgage and you were told what amount you qualified for? Many thought, "*Oh, I must be able to afford that*." Not so fast! How many mortgage owners are feeling the brunt of this now? Did you cross against the red light this morning with hot coffee in your hands and maybe your cell phone too? Was that a risk with oncoming buses and traffic or slippery conditions? The point is, we make decisions that are risk-based all the time, and we do so without considering the consequences because we accept the risk associated with that activity.

As I fly to Los Angeles on a Boeing 757, I am reminded to read the safety card upon boarding. I admit I did not! Instead, I am relying on the diligence and experience of the crew to properly and safely get me to my destination, and I accept the level of risk associated with that decision. Did you know Federal Regulation FAR CFR 121.571 and 121.577[1] requires all passengers to review the safety card and adhere to the crew's instructions? We know – we hear it announced, but are we really paying attention? In an emergency situation, we will perhaps wish we had read the card front to back. And does it make you nuts when an older person with perhaps the appearance of being less than physically fit confirms audibly

Laura H. Goldzung, CFE, CAMS is President and Founder of AML Audit Services, LLC, an anti-money laundering and fraud boutique consultancy specializing in independent testing and compliance consulting services to financial and nonbank financial institutions. Additional expertise includes domestic and international training, design and development of BSA/AML compliance programs, risk assessment and analysis, remediation and corrective action programs, expert witness testimony, and CFPB compliance benchmark assessments.

to the flight attendant that he or she is prepared to assist while sitting in the emergency row? I don't know about you, but I would much prefer the football-sized fellow in front of me to be sitting in the emergency row in case the hatch has to open. Of course, that seat is available only at a premium since the airlines began to monetize all services and add-ons – a mistake for the emergency row, IMHO, but don't get me started on that rant.

In the world of pervasive fraud, it is incumbent upon financial institutions of all types and sizes to assess risk, if only to know what risks exist for them. For many, it takes only one or two incidents to sit up and take notice. But why react when you can simply *proact*? Take the recent cyber-fraud incident at retail giant Target. Did senior management imagine that such a situation could happen at the level that it did? Were they prepared for such an incident? Only Target's risk management team knows for sure, but suffice it to say, this could happen to any number of businesses and it presents the challenge of preparedness and readiness to sufficiently prevent and/or manage such incidents.

In the world of pervasive fraud, it is incumbent upon financial institutions of all types and sizes to assess risk, if only to know what risks exist for them.

Why then do you suppose that many financial institutions ("FIs") resist assessing their risk? As an independent consultant navigating the AML/Anti-Fraud waters with financial services clients of varying types and sizes, I can tell you that many FIs do *not* perform a risk assessment or conduct an analysis of risk in their organization. For the non-bank broker-dealer, do you think it is because risk assessment is not mandated under FINRA regulation and therefore is overlooked or under-emphasized? Or is it that many firms simply do not believe that money laundering and fraud can ever happen to them? I hear that a lot in the field. It is not surprising then, to read about AML program failures and enforcement actions of varying types. Writing a check for the cost of such incidents isn't the answer; rather, having a thoughtful and comprehensive risk assessment in harmony with an effective system of controls will serve to protect the firm in the short and long term.

In the absence of law or regulation, or even expectation, the assessment of risk is anecdotally the first commandment for developing an AML program – laying the foundation for the system of controls and policies and procedures required under the regulation.[2] As a best practice, assessing risk lays the foundation for the system of controls that will drive the AML compliance program. In some sectors, even regulatory expectation will compel a non-bank financial institution to assess risk. This is not the case with FINRA firms however, as FINRA does not have an expectation that you'll have a written risk assessment.

Ever think about the foundation of your house? How about when last year's Super Storm Sandy hit the northeast and all those beach homes collapsed? The remediation is still underway today in the garden state of New Jersey and it now includes measures against the risk of it happening again. It stands to reason, that without a strong foundation, the walls of a house would simply not have the integrity, durability, and strength to hold up under any number of likely or impactful scenarios – weather driven or not.

Conducting a risk assessment will no doubt reveal a variety of risks that influence your AML compliance program development – from the creation of the system of internal controls, types and frequency of training and education, gauging the need for resources whether human or technological, types and number of business processes required to support the infrastructure, need for legal, compliance and other professional advice, products and related services, the geographical jurisdictions you service, the customers and markets with whom you conduct business, vendors and third-parties you engage, employees you employ, the operations and facilities you work from, deployment of capital – and the list goes on. And the variety of risks to assess is no less exhaustive, but typically begins with customers, geographies, products and services. Be sure though to assess the AML compliance program based on outcomes from independent testing, KYE, as knowing the risks your employees present is important to measure, cyber fraud risk if you have e-commerce capabilities, as well as other risk factors. Understanding the risk profile of the firm is a great starting point … in fact, a critical point. Let's break down the essentials.

Where to Begin to *Proact*

There is available guidance on the topic of risk assessment that was produced for depositary institutions assembled by the Federal Financial Institutions Examination Council (FFIEC), a group of regulatory bodies who issued a Bank Secrecy Act/ Anti-Money Laundering Examination Manual. While this manual is considered to be the gold standard by which BSA/ AML compliance programs are based, it is thought that it's strictly for banks. Not to be easily dismissed, I see many non-financial institutions use this manual as a reference to understanding further their AML compliance obligations and as a go-to reference for supplementary guidance.

Alas, there are other good resources. Consider FINRA Rules 3012 and 3130 that require all member firms to perform an annual review of supervisory systems to assure that there are processes in place to prevent and detect violations of applicable law and rules, culminating in a requirement that the CEO of the firm certify that such processes are in place. This review process can assist you in assembling a risk assessment based on the written system of controls you have in place. Also available is the FINRA Risk Control Assessment[3] (RCA) that was instituted in 2012. That survey can serve as a starting point as well.

According to the FFIEC guidance on risk assessment,[4] understanding both the quantity and quality of risk is an important first step. Firms often will begin by developing a risk questionnaire and ask the business unit managers to assess the risks associated with the firm's products and services and the types of clients who buy them. Product managers assist in responding to a product risk questionnaire; operations may respond to other Services Risk issues relating to such services as ACH and wire transfers, LOAs (internal journals), receipt of securities' certificates, and other operational functions, while new accounts or even marketing can speak to the numbers and risk profile of jurisdictions served – domestically and internationally. And what of the other categories of risk (might) your firm may have? And who are the customers? Sophisticated and aggressive? Inexperienced but frequent? Margin or cash? Speculative or conservative? High net worth or not? Transactional or consultative? It's important to identify how many of what type you serve, so that you have a good idea of the risks associated with each group and to fully understand the level and type of activity you can expect. Let us not forget how suitability plays into AML too.

AML converges with many issues in the broker-dealer setting – just look at the recent enforcement actions around Section 5 of the Securities Act of 1933 and its relationship to AML. Money laundering violations are cited in virtually all cases.[5] Assessing your risk is paramount for some types of business, particularly if you have a large portfolio of higher risk transactions. If, for example, a large percentage of your firm's business is conducted in high risk jurisdictions, it is wise to assess the inherent risk, the mitigations and controls already in place, and the risk remaining to ensure that the firm can withstand that residual risk. What if you conducted business with a high net worth client who resides in Mexico and it comes to light that this client is identified in a money-laundering scheme? Are you confident that you did everything right? You assessed the risk in dealing in a higher risk jurisdiction; you conducted appropriate due diligence on the client; you monitored transactions and investigated red flags; you followed your firm's enhanced due diligence protocols. You did everything right to the best of your ability, there were no indications this client might be laundering money at your institution and yet he revealed himself at another? Can you defend your actions when called by law enforcement to produce documentation?

Let's say your broker-dealer serves sophisticated and high net worth clients, and one morning a client decides to buy a villa in Tuscany and suddenly wants you to wire a few million from his investment account to an unknown third-party abroad. How prepared are you to facilitate this request? Will you allow it? Will you conduct an enhanced due diligence (EDD) process, screen against sanctions lists and conduct a negative news search? Will your clearing firm?

If you have a portfolio of these types of clients with similar demands for instantaneous services, you'll want to assess the specific risk around this activity to determine if your firm will have exposure to any regulatory, operational, credit and/or compliance risk by continually wiring funds abroad, and often to third parties unknown to the firm and possibly the client. The purpose of conducting a risk assessment is to determine what risks exist and how you will mitigate those risks. It only takes a flawed internal process to produce operational risk. All firms must manage operational risk to keep losses within their risk tolerance - the amount of risk they are prepared to accept in pursuit of their objectives. Whether operational, credit or market or even regulatory risk, assessing and understanding tolerance and risk appetite is smart business for any firm.

Here's how that looks using a matrix format:

Table A. Simple Risk Matrix View

Inherent Risk	Mitigating Controls in Place	Residual Risk
The pure risk found in the product, service, customer, geography, before any mitigating controls are implemented	▪ Red flags ▪ Alerts generated by monitoring system ▪ Exception reporting ▪ Periodic activity reviews ▪ Fully documented due diligence including KYC expectations of activity levels	The remaining risk the firm accepts in conducting that business. Demonstrating and documenting diligence around residual risk is what your policies and procedures provide

Additional aspects of assessing risk include the probability or likelihood that a negative or harmful event will occur and the cost or amount of loss or expense that will result from the event. Using our earlier example of servicing high net worth clients, would you consider that excessive wire transfers to unknown third parties might have substantial money laundering and regulatory risks? That will depend on the controls you have in place to mitigate the risk and the risk exposure the firm is willing to accept. First look at Table B to view how you would include additional factors to consider. Is it likely this would happen, and what would the impact be if it did?

History has taught us that sending third-party wire transfers to foreign jurisdictions is high risk. AML compliance professionals also know that even with mitigating controls in place, the residual or remaining risk is still pretty high overall, so assessing the likelihood of it happening and the impact it would have on the firm becomes all too important if you have clients who demand services of this type. Table C provides a simplistic view to assessing the risk of this one service. These tables are for illustration purposes only and serve to demonstrate that assessing risk using a matrix keeps is a well-organized format to begin assembling your document.

Whether you use questionnaires, interviews or other means to identify and collect information on risk in certain areas of the firm, performing the assessment not only sets the stage to identify risk factors – it lays the foundation to more fully understand the risks imposed by these factors. Demonstrating that a judgment is made based on analysis and diligence goes a long way to defending an action taken.

Controls. What do we mean by that? Let's say your firm has a CMA-style account as service to higher net worth clients. Once the debit card and checkbook are issued to the client, what is the firm's AML responsibility? And how about the small BD associated with the large insurance company? Does

Table B: Definitions

Example Risk Types	Inherent Risk	Mitigating Controls in Place	Residual Risk	Impact	Likelihood
▪ Customers ▪ Products ▪ Services ▪ Geographies ▪ Correspondents ▪ Third-Party Vendors ▪ KYE & non-employees ▪ AML Program ▪ Cyber Fraud ▪ Governance ▪ Compliance	The pure risk found in the product, service, customer, geography, or other item before any mitigating controls are implemented	▪ Red flags ▪ Alerts generated by monitoring system ▪ Exception reporting ▪ Periodic activity reviews ▪ Fully documented due diligence including KYC expectations of activity levels	The remaining risk the firm accepts in conducting that business. Demonstrating and documenting diligence around residuals risk is what your policies and procedures provide.	Cost of event can impact regulatory, operational, credit or reputational assets.	Probability that an event will occur.

Table C. Product Risk

Type	Inherent Risk	Mitigating Controls	Residual Risk	Impact	Likelihood
Third party wires to foreign jurisdictions	Extreme	Multiple controls implemented	High	High	Moderate

the "check and app" client – those where the client completes a mutual fund application which the RR forwards with payment to the investment company – directly expose the firm to AML risk? The firm doesn't get a pass just because it is not placing the trade for the client through the firm's automated channels, and is passing payment along to the investment company. The firm must follow its Customer Identification Program verification requirements and KYC requirements, demonstrating its commitment to forming a reasonable belief that it knows the customer as required regardless of how the transaction is processed.

Examiners look for a risk assessment to be "reasonable." A subjective view perhaps, but what it means to the consultant like myself who conducts independent reviews, reasonable means the firm considered its risks following a comprehensive analysis of the risk factors.

Table D is just one illustration of one product. If you performed this analysis across your product/services lines you will have assessed your exposure for all products and services.

One of the missteps of conducting a risk assessment is to limit the assessment to customers, products and services, and geographies. A thorough risk assessment will explore and consider all risk factors and design mitigation controls to be implemented. And that leaves the remaining risk, that which the firm accepts in operating its day-to-day business.

An evaluation of compliance risk exposure takes into account the financial crime risks, the strengths and effectiveness of established controls designed to mitigate risk and the identification of residual risk. The risk assessment is designed by the firm for the firm, to identify potential events that, if they occur, can be managed within the firm's risk appetite.

Preparing a thoughtful risk assessment, no matter how limited in scope, will help the firm as well as key personnel to better understand its risk appetite and its risk exposures based on geographies, customers and products/services. The risk assessment as a foundation for your compliance program can begin with a thoughtful review of operations when completing the FINRA risk control assessment, and is a great starting point. Understanding the risks faced in managing day-to-day operations is key to protecting your assets. Remember that demonstrating knowledge of the firm's appetite for risk will go a long way to defending your program and keeping you out of the headlines.

ENDNOTES

1 http://www.gpo.gov/fdsys/pkg/CFR-2012-title14-vol3/pdf/CFR-2012-title14-vol3-sec121-571.pdf
2 http://www.fincen.gov/statutes_regs/bsa/
3 http://www.finra.org/Industry/Regulation/Guidance/RiskControlAssessment/
4 http://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_005.htm
5 http://www.finra.org/Newsroom/NewsReleases/2013/P314981

Table D. Example of a product offering

Product/Service	Inherent Risk	Mitigating Controls in Place (inclusive of policies, procedures, processes	Residual Risk
CMA-type Accounts (valet, white label programs)	High (Checking, debit card activities including frequency of use, velocity, $ volumes, fraudulent use)	▪ Red flags ▪ Alerts generated by monitoring system ▪ Exception reporting ▪ Periodic activity reviews ▪ Fully documented due diligence including KYC expectations of activity levels	Low