The objective of this white paper is to offer specific considerations and suggestions for how the internal audit department can design a firm-wide AML risk assessment tool that: 1. improves the auditor’s ability to identify relevant AML risks; 2. sets the foundation for thoughtful and supported risk determinations; and 3. produces results that can assist in the development of an audit plan that satisfies regulatory expectations for deterring money laundering and terrorist financing.
# TABLE OF CONTENTS

EXECUTIVE SUMMARY ........................................................................................................................................... 3

INTRODUCTION ........................................................................................................................................................... 3

  Regulatory expectations are high and the auditor’s role is evolving................................................................. 3
  The audit plan reflects whether Audit is “on track” in the eyes of the regulators.............................................. 5
  Audit’s risk assessment process drives the audit plan .......................................................................................... 5
  There “is” a difference between an Audit AMLRA and other AML risk assessments ........................................ 6
  Assumptions ............................................................................................................................................................. 7

DEVELOPING AN AUDIT AML RISK ASSESSMENT TOOL .................................................................................. 7

  Overview ................................................................................................................................................................. 7
  A closer look ............................................................................................................................................................ 8

THE SUPPORT FRAMEWORK: Investing in Audit’s risk assessment process ...................................................... 25

INTERPRETING AND USING RESULTS: The audit plan and beyond ................................................................. 27

TAKEAWAY: The risk assessment “design” can better equip Audit ....................................................................... 28

APPENDICES ......................................................................................................................................................... 30

  A - Overview of considerations ............................................................................................................................ 30
  B - Examples of considerations ........................................................................................................................... 31
  C - References ....................................................................................................................................................... 35
  D - Helpful resources for rating and scoring ....................................................................................................... 37
  E - Acronyms and terms used throughout this paper .......................................................................................... 37
  F - About the author ............................................................................................................................................. 39

The views expressed in this paper are those of the author, and the author alone. The author is not necessarily representing the views or opinions of JPMorgan Chase.
EXECUTIVE SUMMARY

For reference purposes herein, Bank Secrecy Act (“BSA”), anti-money laundering (“AML”), Office of Foreign Assets Control (“OFAC”) and sanctions will be referred to collectively as “AML.”

The primary objective of this white paper is to offer specific considerations and suggestions for how a financial institution’s internal audit department (“Audit”) can design a firm-wide AML risk assessment (“AMLRA”) tool that: 1. improves the auditor’s ability to identify relevant AML risks; 2. sets the foundation for thoughtful and supported risk determinations; and 3. produces results that can assist in the development of an audit plan that satisfies current regulatory expectations for deterring money laundering and terrorist financing.

Internal audits are critical for proactively identifying deficiencies and for ensuring that financial institutions (“FIs”) maintain AML functions and programs that are aligned with supervisory requirements and examiner expectations. The selection of these audits — as represented by an audit plan — is the primary roadmap for AML testing activities and is often determined by a risk assessment. A notable challenge relating to the compilation of an audit plan that effectively captures AML risk lies with the initial design of the risk assessment tool\(^1\), which should, at a minimum, produce meaningful results that the audit department can interpret, analyze and use to build an appropriate risk-based plan.

Most FIs that perform a wide range of activities across a number of separate business lines, legal entities and jurisdictions have — or are expected to have — a risk assessment process that can assist with their audit planning. The degree to which this process focuses on AML and complies with regulatory expectations varies from institution to institution.

The content provided herein is intended to offer guidance for enhancing or constructing a risk assessment tool that delivers helpful direction to the audit department in evaluating its FI’s AML risks and controls, as well as in documenting decisions. This white paper is not intended to detail the complete process of a risk assessment, but rather to describe how to work within Audit’s existing risk assessment framework to ensure that the AML component is developed and represented appropriately. A strong and well-designed tool should equip the auditor to identify risk and to demonstrate and evidence how risk ratings and related conclusions were derived.

*The views expressed in this paper are those of the author, and the author alone.*

INTRODUCTION

Regulatory expectations are high and the auditor’s role is evolving — The requirements for AML compliance programs and related internal AML controls have remained, for the most part, consistent with past regulatory statutes and guidance such as the BSA [12 CFR 21.21] and the USA PATRIOT ACT [section 352]. However, within the past five years, the financial services industry has experienced noticeable changes in the articulation of regulatory expectations regarding the adequacy and overall view of internal controls. Concurrently, there has been a significant increase in both the frequency and severity of enforcement actions among the world’s largest and most reputable financial corporations. Advances in technology and an expansion of sophisticated products and delivery systems may be partially responsible for the changing environment. These developments have not only provided additional banking opportunities but have also resulted in more complex financial relationships and have compelled money launderers to become smarter and more creative. Nonetheless, despite the

\(^1\) The term “tool” will be used herein to represent the mechanism (such as a basic template or system) used by the FI to organize, record, assess and rate AML risks. The tool can be a sophisticated system or a simple spreadsheet, as well as any accompanying guidance.
many possible impetuses for the increased legal force, it is clear that there has been a shift in the accepted standard for sound banking practices.

Between the years 2010 and 2013, there have been over twenty-five AML-related consent orders, written agreements and cease and desist orders and more than $900 million in fines. According to a report issued by the U.S. Senate, recent prosecutions and legal actions relating to OFAC violations between 2010 and 2012 have amounted to over $1.4 billion, involving well-known financial institutions. Based on metrics from the U.S. Department of the Treasury, OFAC-related penalties and settlements between January 2, 2013 and October 25, 2013 totaled $12,875,278. In a recent industry paper, Kenneth Simmons analyzed BSA examination results of 137 financial institutions that were issued reports between September 2009 and March 2013; these results reflected that, as of April 2013, there were more than 202 open Matters Requiring Attention (“MRAs”) that related to the four pillars of an AML program (audit, internal controls, training and the BSA officer). Of all MRAs reviewed, 83.88% of outstanding MRAs referenced internal control failures.

Based on a review of regulatory orders in 2012 and 2013, frequently cited AML program weaknesses included:

- Inadequate customer due diligence and enhanced due diligence practices.
- Incomplete identification of high-risk customers.
- Insufficient policies, procedures and training.
- Failures in monitoring and identifying suspicious activity.
- Poor reporting and filing practices relating to suspicious activity.
- Ineffective independent testing and audit functions.

The underlying message suggests that the expectation for FIs to be less reactive and more proactive (e.g., by enhancing risk management practices and maintaining an effective regime to audit their AML compliance programs) has become a minimum standard in the eyes of supervisory agencies. This includes further attention to:

- A risk-based approach that focuses on higher-risk clients, products, services, geographies and relationships
- Timely identification of deviations from policy, laws, rules and regulations within individual business lines and across businesses and activities
- Testing the adequacy of internal controls designed to ensure compliance with AML requirements

As part of this enhanced scrutiny, regulators are emphasizing the importance of independent testing and the evolving role of the AML auditor in helping their FI to manage risk and sustain an operational AML program, such as through additional focus on risk tolerance, the level of assurance, the depth and precision of controls, the nature of substantive testing and the degree of credible challenge. Consequently, Audit has become even more critical in positioning its FI to avoid compliance, legal and reputational risks relating to AML functions.

---

3 See the Minority Staff of the Permanent Subcommittee on Investigations report dated July 17, 2012 entitled “U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History.”
In addition, Audit’s role and its relationship with regulators may be important for another reason. Due to the strong focus on AML and the extent of related challenges within the financial industry, the need for a collaborative approach to combat money laundering and terrorist financing has become more apparent. As such — subject to a reasonable level of comfort that the audit department is effective, competent and dependable — examiners may gradually expand their reliance on the work of AML auditors. This “trust” would be mutually beneficial for both parties.

The audit department is the last line of defense. Audit is responsible for conducting an objective evaluation of the AML compliance program for soundness, adequacy and sustainability while maintaining independence from compliance and business functions. This includes a review of the FI’s risk assessment for reasonableness given the FI’s risk profile (e.g., products, services, customers, entities, geographic locations).

The audit plan reflects whether Audit is “on track” in the eyes of the regulators — In order to meet regulatory expectations and comply with fiduciary responsibilities, Audit is responsible for assembling an audit plan that demonstrates its organization’s knowledge of its Business Units6 and an understanding of the business’ associated risks. The audit plan dictates what areas will be tested in order to ensure that the FI is protected by way of controls that are operating effectively. If the plan is lacking, the FI may be exposed to control gap risk or breaches in regulatory compliance. A sufficient plan should, at a minimum, focus on the highest-risk areas to ensure that either the FI has a sound control environment or that the assessed risks do not pose a significant threat. The cornerstone of an adequate audit plan is a strong risk assessment tool.

Audit’s risk assessment process drives the audit plan — Without a proper risk assessment, it would be particularly difficult for a large, complex, multinational FI to figure out what to audit. An audit plan that includes every possible auditable Business Unit is arguably not a “plan” and is most likely an unrealistic approach in a world of finite resources. The audit department is expected to select audits using a risk-based approach that provides a reasonable belief that critical risks — such as those relating to money laundering and economic sanctions — are identified and assigned adequate testing coverage in a timely fashion. As such, a successful risk assessment should result in a detailed risk profile for each Business Unit, which can subsequently drive the level of audit coverage, including both scope (e.g., extent of testing areas/testing steps) and frequency (e.g., annually, bi-annually). Further, a well-documented and thorough assessment can supply the rationale for including or excluding a specific audit area. The process of building the audit plan should involve consideration of existing or prior audit coverage, unique business risks, pre-existing issues and the severity of AML risk factors.

OVERVIEW OF PRIMARY AUDIT OBJECTIVES

✓ Determine whether the overall AML/BSA compliance program is suitably designed and operating effectively.
✓ Identify any material program weaknesses, control deficiencies and corresponding opportunities for program, process and control enhancements, and report them to senior management and the board (usually the audit committee).
✓ Assist management with identifying money laundering, terrorism financing and other financial crime vulnerabilities.
✓ Perform and document procedures and results that may be useful to regulators in conducting their supervisory examinations.
✓ Assess and identify possible gaps and opportunities for management to continually improve its suspicious activity detection, investigation, analysis, escalation, documentation and reporting processes and controls, including due diligence feedback and the enterprise-wide AML risk assessment process.
✓ Assess management’s AML strategic planning process.
✓ Identify opportunities and methods to help management make program enhancements continuous and sustainable.
✓ Assess and identify opportunities to enhance management’s self-monitoring and self-testing compliance review program.
✓ Assess how well AML compliance is integrated into the business.

Adapted from: The SAR Activity Review — Trends, Tips and Issues (Issue 16), (October, 2009).

---

6 For the purposes herein, all auditable business areas, control functions/utilities and lines of businesses (“LOBs”) will be referred to collectively as “Business Units.”
There “is” a difference between an Audit AMLRA and other AML risk assessments — Most risk assessment exercises have the common objective of identifying and assessing risk with the purpose of determining how to prioritize and focus resources based on the areas of most concern. Differences between risk assessment tools do exist, however, and these may be attributed to “who” the tool is designed for and “how” the results will ultimately be used. The design sets the stage for what the output will look like, and as such, both the “who” and the “how” are important considerations. Understanding this distinction at the onset will facilitate the development of the risk assessment tool.

An Audit AMLRA, for instance, targets different information from a line of business (“LOB”) AML risk assessment. LOB AMLRAs are usually approved by the AML officer or other AML department designee and the predominant objective is to identify and assess AML risk with the purpose of resolving issues, driving institutional activities, allocating resources and informing risk-based business decisions. These decisions could include whether to exit relationships with particular client types, whether to eliminate particular products or services, or whether to expand upon the control environment.

The predominant objective of an Audit AMLRA — usually completed by an auditor or other audit department designee — is to identify and assess potential risk (e.g., control gaps) with the purpose of constructing a standalone AML risk assessment that can pinpoint areas warranting either immediate escalation (such as a blatant difference in how Audit has perceived a risk versus the business line’s view) or areas warranting further substantiation and testing. By conducting a more detailed review (an audit) of less apparent areas, the department is able to perform independent evaluation, substantiate concerns and communicate issues to the relevant business area(s) for them to take appropriate action. Audit may also risk rate control gaps and weakness to assist the business with prioritizing and planning its activities. Accordingly, it may be more reasonable to expect the Business Units to derive statistics and pull information from business-specific metrics or reports as part of its LOB AMLRA, while an Audit AMLRA may reflect a combined approach of independently deriving some pieces of information and leveraging other pieces, such as by discussing preexisting information from prior risk assessments (e.g., country, client, LOB, product) or material from previously identified issues (e.g., audit, regulatory) 7.

Likewise, a firm-wide customer risk assessment process is generally conducted by the business line, compliance or risk departments and focuses on determining which individual customers should be ranked as high-risk (“HR”) based on the firm’s approved customer risk rating model. When Audit conducts an assessment of customer risk for audit planning purposes they are likely interested in assessing the aggregate level of customer risk within a particular business area, and thus it makes sense for an Audit AMLRA to focus on determining the proportion of customers that are categorized as HR as per the existing firm-wide customer risk assessment.

Ideally, an effective Audit AMLRA should assist with audit decisions relating to: a) whether the FI’s risk assessment processes are effective; b) what Business Units should be audited; c) what AML components within a Business Unit

---

7 While the business’ risk assessments and corresponding data should be tested as part of a comprehensive Audit program, it may not always be feasible to substantiate and independently validate all pieces of information as part of the Audit AMLRA process due to timing constraints, such as annual planning deadlines, and other challenges, including a large volume of assessments requiring completion by Audit. As such, rather than testing all referenced firm-wide risk assessments (country, client, LOB, product, etc.) and independently deriving all information used for the Audit AMLRA, the Audit AMLRA may be conducted more efficiently at the risk assessment stage by allowing for some level of reliance on existing information when drawing conclusions. In these instances, Audit should have a reasonable level of comfort that the leveraged information is accurate and/or reliable (such as through previous validation exercises). Although not encouraged, in situations where Audit may reference or leverage information that has not been previously verified — or that relates to known issues or concerns — Audit should document this and flag for subsequent substantiation and testing. If for instance, the Audit AMLRA relies on the product risk assessment for support that remote deposit capture is a HR product and then relies on the LOB risk assessment for support that 50% of customers within Retail Banking use remote deposit capture, then Audit may want to consider separate audits for both the product and LOB risk assessments to support its inferences.
may warrant testing coverage; d) the frequency for which a Business Unit may need to be tested; e) prioritization and timing of audit coverage across Business Units; and f) potential resourcing demands for conducting the resulting audits.

The sharing of Audit’s AMLRA results with the business line may be a win-win gain. The audit department may want to consider whether it makes sense to establish a vehicle for sharing relevant results with the business and, if so, under what circumstances. Certain findings, such as differences in opinions, potential testing areas, open questions regarding specific data or otherwise helpful information, may on occasion serve useful to provide sooner rather than later to assist with clarifying issues, resolving discrepancies and expediting corrective action.

**Assumptions** — The guidance provided herein is based on the following assumptions:

- The audit department has an existing risk assessment process for its annual audit planning.
- The audit department has an existing scoring model/methodology (e.g., definitions, weightings, numerical criteria).
- For each Business Unit within the FI, there are one or more individuals within the audit department who understand the business and are familiar with the business’ unique risks.
- The audit department has one or more AML subject matter experts and/or would be willing to hire additional AML resources.

**DEVELOPING AN AUDIT AML RISK ASSESSMENT TOOL**

**Overview** — The development of a robust risk assessment model is largely, if not completely, dependent upon the individual elements that are chosen as the risk and control environment factors to be assessed and evaluated. Based on the Federal Financial Institutions Examination Council (“FFIEC”) and other leading industry sources, there are certain categories of inherent AML risk that apply broadly across the financial industry and are universally accepted as standard risks that must be addressed. As explained by the Federal Deposit Insurance Company (“FDIC”), “[i]nherent risks are the risks that exist before the application of controls intended to mitigate those risks. Clearly identifying inherent risks is particularly beneficial in making determinations for the scope and frequency of audit and independent reviews—determinations that should be based on a financial institution’s assessment of inherent risk without assuming that controls are functioning as intended. Residual risks are those that exist after the application of controls. In this context, risks cannot be completely eliminated, even though layered security may reduce risk to an acceptable level.”

Primary inherent AML risks relate broadly to an FI’s:


Pursuant to an FI’s obligation to maintain an adequate AML compliance program, FIs are expected to establish a control environment that minimizes and — where possible — safeguards against AML risks. From an Audit

---

8 See Appendix D for helpful resources for rating and scoring.
10 See “From the Examiner’s Desk: Customer Information Risk Assessments: Moving Toward Enterprise wide Assessments of Business Risk.”
perspective, when evaluating an individual Business Unit’s control environment, the audit department should, at a minimum, assess the current state relating to:

- Know Your Customer Practices.
- Suspicious and/or Unusual Activity.
- OFAC and Sanctions.
- Employee AML Expertise and Coverage.
- Management and Oversight.
- Policies, Procedures and Processes.
- Operations and Technology.

According to the Association of Anti-Money Laundering Specialists ("ACAMS")\(^{11}\), commonly cited risk assessment weaknesses by regulatory authorities include: a) assessments were not performed and/or not evidenced through documentation; b) assessments did not include all lines of business or entities; c) assessments did not consider all major risk categories; d) there was a lack of methodology for assigning risk ratings/levels; and/or e) policies and procedures were not commensurate with the institution’s risk profile. The following sections will explore the art and science of forming a well-crafted AML risk assessment.

Auditors and regulators may be considered the primary audience. The two key players who will be using the tool the most are the auditor completing Audit’s assessment and the AML examiner evaluating Audit’s assessment. This is a helpful consideration when designing the tool.

A closer look — At the very least, an ALMRA tool should be conducive to the identification, quantification, assessment and documentation of the level of risk within a Business Unit. A strong design leads, directs and guides the auditor’s focus and helps the auditor to successfully execute these functions while avoiding generalizations. By highlighting key focal points and providing clear descriptions and examples of pertinent risk and control considerations within the design of the tool itself (e.g., the template completed by the auditor or accompanying guidance), the tool can pave the way for a more efficient assessment that reflects stronger quantitative and qualitative analysis.

The following section is a high-level illustration of relevant considerations that can be incorporated into, or addressed as part of, the design to improve the consistency and quality of risk assessment results — including better narratives (e.g., written rationale, executive summaries) and more detailed evaluations of the relevant Business Unit(s). While the following elements do not represent a restrictive list, the framework is intended to broadly capture all facets of an AML program and serve as a comprehensive set of considerations with the flexibility to address additional items that may not be specifically mentioned herein.

\(^{11}\) See “Spotlight on Large Institutions: Conducting Enterprise-Wide AML Risk Assessments that Go Beyond the Expectations of Examiners and Senior Management,” ACAMS; June 26, 2013.
Inherent Risks

The process of identifying and assessing the degree of inherent risk within a Business Unit will help to quantify the extent of residual risk, which in turn can inform audit planning decisions such as whether to include a Business Unit in the annual plan, and if so, at what testing frequency and scope.

Potential inherent risk areas include, but are not limited to:

Customers — Certain customers may pose a higher risk of money laundering and/or terrorist financing with respect to unique characteristics, such as the nature of their business (for legal entities), their occupation (for individuals), the duration of the relationship with the FI and/or the number of accounts across various business lines. The focus of Audit’s assessment should be on identifying the extent to which the Business Unit’s customer population reflects high-risk characteristics based on the risk attributes that have been considered.

Potential considerations for assessing the level of risk (i.e., high, medium, low) include:

- **HR Customer Types** — Most large multinational FIs maintain compliance-approved lists that reflect the FI’s agreed upon categorizations for HR customer types. This commonly includes particular industries/occupations (e.g., small arms manufacturing, used car dealers) or other designated customer categories that may require special due diligence (e.g., non-governmental organizations, bearer share entities, money services businesses and foreign exchange houses, third-party payment processors, politically exposed persons ("PEPs")). An appearance on such a list does not necessarily indicate that the customer should be treated as a HR customer; however, it does suggest that the customer has one or more HR characteristics that warrant further consideration. The final decision to assign a HR rating is generally governed by a separate customer risk assessment model that considers a variety of customer-specific factors such as location, products used, ownership attributes, the presence of anti-money laundering systems, extent of regulatory oversight and/or material negative information (e.g., associations with enforcement actions, sanctions, criminal activity, government inquiries, known money laundering). When evaluating a particular Business Unit’s customer base, it may be helpful to consider both the FI’s assigned risk rating for the customer as well as other individual risk factor components that may influence AML risk.

- **Duration of Relationship** — The length of a client relationship as indicated by account maturity (i.e., based on the date that the first account was opened with the FI) may be an indicator of how well the FI knows its customer. FIs tend to have a better understanding of their customers’ expected activities and behavior when they have had time to observe them and interact with them.

- **Closed/Blocked Accounts** — Frequent bank-initiated account closures and/or account blocks may be indicative of customer characteristics or transactions that are either unexplained, questionable or undesirable.

---

12 According to the FFIEC, “[a] customer is a ‘person’ (an individual, a corporation, partnership, a trust, an estate, or any other entity recognized as a legal person) who opens a new account, an individual who opens a new account for another individual who lacks legal capacity, and an individual who opens a new account for an entity that is not a legal person (e.g., a civic club). A customer does not include a person who does not receive banking services, such as a person whose loan application is denied.” As defined in 31 C.F.R. § 103.121(a)(1), “[a]ccount means a formal banking relationship established to provide or engage in services, dealings, or other financial transactions including a deposit account, a transaction or asset account, a credit account, or other extension of credit. Account also includes a relationship established to provide a safety deposit box or other safekeeping services, or cash management, custodian and trust services.”
Number and Nature of Accounts — Customers who have accounts or access to services across multiple Business Units, as well as customers with accounts that offer enhanced or flexible features (e.g., higher transactions limits, minimal restrictions), may present increased risk exposure due to their ability to conduct a wider range of activities such as those involving additional products/services, delivery channels, locations or account types. These customers may engage in complex, frequent and/or diverse transactions within the FI and may pose additional monitoring and control challenges. In addition, where customers have a footprint across multiple Business Units, there is a higher potential for confusion over accountability and respective responsibilities.

Magnitude provides perspective; be sure to consider context when assessing and documenting statistics and other metrics. The use of quantitative information is instrumental in signaling the quality and credibility of a risk assessment; however, numbers without context are just noise. When collecting, reviewing and documenting metrics for assessing risk, it is important to consider both the absolute numbers and changes in those numbers within the context of the Business Unit, including clear demonstration of the relative significance within the assessment. A certain number of HR customers within one Business Unit may have a very different connotation than the same number of HR customers in another area, depending on factors such as the proportion of the overall population represented. Similarly, two Business Units may have the same number of new customer relationships; however, one of these may have rapidly increased the number of new customers within the past year. Material increases or decreases should be evaluated and documented within the assessment.

Products and Services — Certain products/services pose a higher risk of money laundering and/or terrorist financing depending on the nature of the products/services and the capacity in which they may be used. Particular products/services, for instance, may support a higher degree of anonymity (e.g., prepaid cards, Internet banking, virtual currency), allow for third-party engagement (e.g., remotely created checks [“RCCs”], U.S. dollar drafts) or facilitate the handling of high volumes of currency or currency equivalents across less regulated jurisdictions (e.g., cross-border wire transfers). Products/services traditionally viewed as lower risk may warrant a closer review should they possess modifications or accommodations that allow for higher-risk activity. Likewise, by nature of the products/services offered, a Business Unit itself may pose enhanced susceptibilities due to its inherent “relationship” with a customer (i.e., if the Business Unit has close or personalized interaction with wealthy, influential, or otherwise important customers) or if it is anticipated that significant profit or business may be generated by the Business Unit based on its customer types, such as what might be expected from high-net-worth individuals. The focus of Audit’s assessment should be on evaluating the types of products/services offered (including associated business strategies and relationships) and the extent to which the Business Unit’s customers either use, or have the ability to use, products/services that present high or unique AML risk.

Potential considerations for assessing the level of risk (i.e., high, medium, low) include:

HR Products and Services — Most multinational FIs maintain compliance-approved lists that reflect the FI’s categorizations for HR products/services. This commonly includes particular products/services that are complex in nature or that offer the potential for anonymity, speed or transferability (e.g., remote deposit capture [“RDC”], trade finance, payable-through accounts, prepaid cards, certain types of mobile technology). A greater number of customers that use, or are expected to use, HR products/services within a particular business could present additional challenges in monitoring, understanding and/or detecting AML risks. In
addition, consideration should be given to how products/services are being used and whether there may be unique AML risks that are not otherwise captured by the product/service risk rating. A low- or medium-risk product/service may present higher AML risk depending on particular characteristics, modifications or the overall capacity in which the product/service may be used (e.g. automated clearing house ["ACH"] transactions may not necessarily be rated as HR, but these transaction may offer the opportunity for unidentified non-customers to access the FI’s internal systems). In general, the potential for non-HR products/services to be used as a conduit for money laundering is higher in environments where controls are conventionally loose or altogether absent.

**New Products and Services** — A Business Unit with a greater number of new products/services may pose a higher risk than a Business Unit with more established and familiar products/services that have been previously evaluated, monitored and/or used. Products/services with shorter shelf lives tend to present a higher degree of uncertainty as to how each product/service may be used and the subsequent potential for misuse.

**Degree of Business/Sales Generated from HR Products and Services** — Although a Business Unit may not offer a significant number of HR products/services (or have a significant number of customers who use HR products/services), this does not necessarily negate the risk of having a relatively high amount of revenue generated from the use of HR products/services. A smaller concentration of customers with enhanced usage or large-dollar-value transaction activity deriving from HR products/services may also be an indicator of AML risk.

**Risk Tolerance and Business Strategies** — Business Units with a higher tolerance for risk are inherently more risky, regardless of the controls that may be in place. Indicators of a high-risk appetite might include: a willingness to accept higher-risk customers or to provide HR products/services, expansion of products/services into riskier jurisdictions, lax commitment to implementing critical AML processes or controls (e.g., through an approval or exception process that allows the Business Unit to deviate from normal protocol) or radical and frequent changes in business strategies.

**Transaction Activity** — Certain transactional behavior and patterns, such as a high volume of transactions, large aggregate dollar amounts of activity or transactions entering and leaving accounts at high speeds (also known as “velocity”), may warrant further attention as money laundering and/or terrorist financing often involves transaction activity characterized by complex flows, higher speeds and sometimes larger dollar amounts so as to obscure audit trails of select transactions and accumulate sufficient funds to support criminal intentions. In addition, a high volume of transactions involving HR jurisdictions, transactions involving indirect customers and/or otherwise unexplained or unreasonable behavior may be indicative of potential money laundering and/or terrorist financing. The focus of Audit’s assessment should be on evaluating the transaction profile for the Business Unit and the extent to which the Business Unit reflects transaction activity that may be indicative of enhanced AML risk.

---

13 According to the International Organization of Supreme Audit Institutions (INTOSAI), "[r]isk appetite is the amount of risk on a broad level that an entity is willing to accept in seeking to achieve its objectives. It reflects the risk management philosophy and in turn influences the entity’s culture and operating style. Risk appetite can be considered quantitatively or qualitatively. It should be considered in strategy setting, where the desired return from a strategy should be aligned with the risk appetite, that is the willingness to accept or tolerate risk...[r]isk tolerances are the acceptable levels of variation relative to the achievement of objectives. They can be measured through performance targets. Often performance targets are best measured in the same units as the related objectives. Operating within risk tolerances provides management greater assurance that the entity remains within its risk appetite and will achieve its objectives.”
http://www.issai.org/media/13341/intosai_gov_9130_e.pdf
Potential considerations for assessing the level of risk (i.e., high, medium, low) include:

- **Activity Involving HR Products/Services** — A Business Unit with a high overall volume and/or dollar value of activity involving products/services that are considered to be HR by the Business Unit may pose higher risk than a Business Unit that reflects less activity involving HR products/services. In certain circumstances, an increase in the absolute volume and/or dollar value, as well as an increase in the overall velocity of HR and non-HR transactions, may be indicative of enhanced AML risk. Consideration should also be given to the dollar value size of individual transactions involving HR products/services and the total number of accounts (and any identified increases in the number of accounts) within the Business Unit that involve HR activity as described above.

- **International Activity** — A high absolute level (e.g., volume) and/or high absolute amount (e.g., dollar value) of international activity and/or significant increases in either the volume of international transactions or the dollar value of international transactions may present additional money laundering and/or terrorist financing risk as particular countries may be more vulnerable to money laundering and/or terrorist financing due to lax or non-existent controls, laws and/or regulations. International activity includes cross-border and intra-country activity involving international jurisdictions.

- **Transactions Involving Indirect Parties** — Transactions involving parties who are not customers of the FI or transactions routed through third parties pose additional challenges in monitoring, understanding and/or detecting AML risks, as there is no direct relationship with the FI. This may occur when customers are correspondent banks that provide access to third-party foreign financial institutions through nested accounts or where the customer is a third-party payment processor (such as PayPal or Amazon) that provides payment processing services to merchants and other business entities that do not have a relationship with the FI. As such, due to the absence of information surrounding these often unidentified persons, it is more difficult to identify, understand and assess their behavior.

- **Reportable Transaction Activity** — Activity reports are effective mechanisms for identifying potentially suspicious, questionable or unreasonable customer behavior. A Business Unit that reflects a significant level of reportable transaction activity may pose a higher risk than a Business Unit that does not exhibit such behavior. Transaction activity reports include suspicious transaction reports (“STRs”), suspicious activity reports (“SARs”) and other related reports such as currency transaction reports (“CTRs”).

**Geographic Presence** — There are certain jurisdictions that are recognized as being more susceptible to money laundering and/or terrorist financing based on their potential to facilitate the movement, concealment and use of illicit funds. Geographies characterized by weaker regulatory environments, higher levels of corruption, legal uncertainty and political and economic instability, for instance, present difficulties in detecting and deterring illegal operations. An extensive amount of work has been performed by established and internationally recognized organizations (e.g., OFAC, Financial Crimes Enforcement Network [“FinCEN”], Financial Action Task Force [“FATF”], Transparency International) to evaluate and risk rate countries based on their capacity to foster money laundering. Available informational sources and lists include the FATF Black List; the Section 311 designated countries list; Specially Designated Nationals (“SDN”) and Blocked Persons List; countries subject to OFAC sanctions; offshore financial centers (“OFC”); high-intensity drug trafficking areas (“HIDTA”); high-intensity financial crime areas (“HIFCA”); as well as other non-U.S. lists. In addition, many FIs with an international presence tend to have a process in place for leveraging and consolidating the available country risk information to develop their own internal country lists that are then tailored for their specific organization. The focus of Audit’s assessment should
be on evaluating the extent to which the Business Unit is involved with higher-risk jurisdictions as indicated by the FI’s pre-existing country risk ratings.

Potential considerations for assessing the level of risk (i.e., high, medium, low) include:

- **Customers in HR Locations** — A significant number of customers with a known presence in a HR location may pose increased money laundering and/or terrorist financing risk due to their ability to accumulate and route funds through less secure regions. A presence may be inferred by an operating address, a residential address or any other known address that may be indicated in the customer’s profile.

- **Physical Presence in HR Locations** — The extent to which a Business Unit is involved with HR jurisdictions may, to some degree, be reflected by whether the Business Unit has access to a physical operating branch or legal entity within a HR jurisdiction.

- **Transactional Activity with HR Locations** — The extent to which a Business Unit is involved with HR jurisdictions may, to some degree, be reflected by the number of customers who exhibit frequent transactions within HR jurisdictions and/or the number of customers with account features or products that indicate activity with foreign locations (e.g., cross-jurisdictional wire transfers, international ACH transactions).

You might not own customers or products, but look deeper for potential AML risk. Not all AML risks may be identified through the same lens. Each Business Unit has different risks depending on its activities and how business is conducted. AML risk might be more apparent for Business Units that directly own customers, such as an investment banking division; however, for other areas such as technology, proprietary trading desks or Business Units that sell or develop products on behalf of other businesses, it may be less obvious as to how inherent risks should be identified, rated and discussed within the AMLRA.

In these instances, it helps to consider transactional activity (e.g., with vendors or counterparties) and to think holistically about the Business Unit’s “potential” (e.g., in the absence of controls) to influence AML Risk, such as whether the Business Unit affects risk in other business areas within the FI. A technology function, for instance, may provide AML data to a retail business to assist them in understanding its customer segmentation. If this data is incorrect and subsequently relied upon, it may lead to unintended business decisions, such as onboarding additional HR customers. Likewise, if a Business Unit’s KYC system experiences lost or altered customer information as a result of a request for the technology function to implement system updates, customers may wind up with inaccurate risk ratings or improper due diligence. An assessment that is attentive to “potential impact” and considers risk in isolation of the control environment can help to draw out those less obvious inherent risks.
Control Environment and Risk Mitigants

A well-designed risk assessment tool should demonstrate that a strong control environment is a continuous feedback loop of interconnected areas within the AML program requiring ongoing and enterprise-wide evaluation.

Potential control environment areas include, but are not limited to:

Know Your Customer ("KYC") — KYC encompasses all practices relating to the collection, review and verification of customer information. The process of gathering information is an ongoing risk-based cycle that begins with verifying the customer’s identity and obtaining a preliminary understanding as to the potential risks associated with the customer. This initial risk profile, which includes customer details such as identifying information (e.g., legal name, address, government identification number) and basic due diligence (e.g., customer type, anticipated activity, name screening results) is often used to risk rate the customer (i.e., high, medium, low) in accordance with the FI’s customer risk scoring methodology. The relationship between customer information and perceived risk is bidirectional — customer details inform the level of risk and the level of risk governs the extent of required customer information.

The essence of KYC is to enable the FI to form a reasonable belief as to the identity of the customer and to obtain an understanding over the customer’s expected behavior, including the ability to identify abnormalities. The information accumulated through this process feeds and informs all pillars of the AML program and, as such, policies, procedures and processes should be in place for obtaining, validating and updating customer information in a manner that allows for effective detection, monitoring, investigating and reporting of suspicious activity. KYC requirements and functions, including customer identification programs ("CIP"), customer due diligence ("CDD"), enhanced due diligence ("EDD") and special circumstances due diligence should be clearly defined and aligned to customer attributes and risks. Enhanced or specialized customer due diligence practices (e.g., for correspondent or private banking accounts) should be in place for customers who pose increased or unique AML risks. The focus of Audit’s assessment should be on evaluating the strength of the Business Unit’s KYC practices, its ability to collect and maintain complete and relevant information; and the capacity to use this information to make appropriate decisions regarding the level of customer risk.

Potential considerations for assessing the strength (i.e., strong, adequate, weak) of the control include:

 Exceptions or Waivers — Throughout the financial services industry, there has been increased focus on developing internal policies, procedures and/or standards that promulgate a consistent and comprehensive approach to conducting KYC. Although deviations from agreed upon practices may be reasonable in specific circumstances, a significant number of exceptions or waivers may pose additional challenges in maintaining adequate and consistent information and may weaken the control environment. In addition, the nature of the exception or waiver may play a role in the level of risk. For instance, relevant characteristics such as the duration (temporary versus permanent), the location (high-risk country versus low-risk country) or the scope (one-off or across a particular group) should be considered when assessing the risk. As a best practice, a process should be in place to ensure that exceptions, waivers or deviations are approved, documented and supported. In instances where temporary exceptions or waivers are permitted, formal tracking and follow-up processes (e.g., automated flags or reports) should be in effect.
Reliance — Reliance on other Business Units or third parties to perform KYC processes or to provide customer information is at times appropriate. This might apply to instances where a customer has an account with another Business Unit that maintains KYC, or where a central utility executes KYC functions. Despite the value in leveraging pre-existing resources, the opportunity for oversight or deficiencies in maintaining adequate customer information may arise in instances where a Business Unit does not fully own the process or possess proper management controls. Extensive reliance (particularly in instances where governance over the reliance is weak) may diminish the Business Unit’s ability to demonstrate that it understands its customer. Instances involving reliance should be documented, approved and monitored to ensure that the Business Unit is effectively managing KYC and is aware of relevant risks. Supplemental measures on the part of the business, such as an oversight program that includes quality control checks or monitoring processes to supervise and report on the activities performed by other Business Units or third parties can help to maintain sustainability and minimize reliance threats.

Completeness of Customer Information — Customer profiles that lack the required KYC components fail to adequately represent the customer and may result in inaccurate risk ratings. A misalignment between the customer’s current risk rating and the available KYC information can hinder the Business Unit’s ability to understand the customer and identify risk. Frequent or repetitive occurrences of customer accounts with incomplete or deficient information may indicate systematic weaknesses in the KYC process.

Renewals, Updates and Periodic Reviews — Performing periodic risk-based renewals and maintaining up-to-date customer information are critical components of understanding the customer base. This involves looking for changes in KYC information (e.g., expected account activity, employment or business details, business ownership, etc.) as well as being cognizant of HR activity in low risk accounts. Customer profiles with outdated information may indicate additional risk exposure as there may be instances where a customer’s risk rating should be elevated and/or additional information collected. Best practices include updating customer information and reassessing customer risk ratings in accordance with established policies and procedures.

Customer Name Screening (see the “OFAC and Sanctions” control section for details on OFAC screening) — An essential aspect of “knowing your customer” lies with performing customer name screening and list comparison searches. This function usually occurs at account opening and renewal stages and includes the identification of PEPs, customers who may appear in section 314(a) search requests, customers who are subjects of adverse information or customers who appear on internal “bad guy” lists (e.g., customers with whom the FI may not want to conduct business). Processes for continual screening of customer names against relevant internal and external databases or lists should be in place. In addition, policies and procedures should, at a minimum, define material versus immaterial matches, articulate the screening process (including escalation or referral points) and clearly indicate expected screening requirements by customer type and related parties (e.g., beneficial owners, authorized signers, powers of attorney, persons with authority to influence the account or respective funds). Where automated screening mechanisms are employed, at a minimum, testing procedures should be documented and followed, and algorithms, such as fuzzy logic, should be supported (e.g., rationale for how threshold levels were selected). As a best practice, internal and external sources (e.g., LexisNexis, World-check, Internet searches) should be accompanied by instructions for usage and reviews should be conducted (and documented) periodically to confirm that practices are consistent and that data sources remain effective and reliable. In instances where this function is performed by a central screening unit or equivalent utility, auditors (through discussions with the business) should illustrate an understanding over the control environment and discuss additional considerations, such as the risk impact of a control failure or the degree of communication between the business and the central screening unit.
**Potentially Suspicious and/or Unusual Activity** — FIs are required under the BSA to monitor, detect and report suspicious transactions. As such, FIs are expected to be vigilant and to establish formal methods for effectively evaluating customer activity, managing alerts, conducting investigations and determining whether to file a SAR or an STR (non-U.S. suspicious transactions report). This includes recognizing and escalating activity where appropriate. A robust control environment should include well-defined and effective processes for promptly detecting, monitoring, escalating, investigating, decision making and filing potentially suspicious and/or unusual activity (referred to collectively as “PSUA” for the purposes herein). Certain aspects of these functions may apply to the Business Unit and/or separate dedicated areas that specialize in activities, such as monitoring, escalation or investigating. Where activities are fragmented or shared among several areas, all parties should maintain an open and continuous dialogue and the roles and responsibilities among all functions should be clear and established. This allows Business Units to more efficiently share information, reduce redundancies and manage activity that requires attention. In all aspects of the SAR process, controls should be in place to ensure confidentiality and security. The focus of Audit’s assessment should be on evaluating the Business Unit’s ability to comply with regulations and law enforcement requests, as well as its capability for managing PSUA with attention given to technology, processes and controls.

Potential considerations for assessing the strength (i.e., strong, adequate, weak) of the control include:

**Detection and Monitoring** — FIs have a number of channels for which to identify PSUA. At a high level, these include: activities conducted as part of normal operations (e.g., manual monitoring, such as activity observed and referred by employees); activities conducted as a result of law enforcement and government requests (e.g., subpoenas, national security letters, section 314(a) and 314(b) information sharing); and information obtained via surveillance monitoring systems. The Business Unit is responsible for ensuring that it has access to transaction reports and system output as necessary to identify relevant PSUA and satisfy reporting obligations. At a minimum, the following reports should be reliable, complete and routinely available: currency activity reports, funds transfer reports, velocity of funds reports, wire transfer records, monetary instrument reports, large item reports, significant balance change reports and nonsufficient funds reports. Automated monitoring mechanisms and related technology (e.g., commercial products such as Fiserv, Oracle or SAS as well as in-house solutions) are often used to capture, monitor and alert on PSUA on a continuous basis. As a best practice for ensuring that these systems are effective, parameters and filters should be...
How to Build an Audit Risk Assessment Tool to Combat Money Laundering and Terrorist Financing

designed and subsequently tailored to focus on activity that is relevant to the Business Unit and that reflects an in-depth understanding of the customer base.

A periodic review of parameters and filters, including testing for gaps, applying statistical/correlation analysis to results (e.g., to assess for reasonableness), determining whether monitoring scenarios are comprehensive and performing fine-tuning to account for known risks and red flags (e.g., U-turn transactions, activity with sanctioned countries, wire transfers involving financial secrecy havens, transactions involving casas de cambios, unusual fund transfers between related accounts or transactions that exceed pre-defined thresholds) should be in place to further enhance the effectiveness of the monitoring tool(s). In addition, this review should evaluate the appropriateness of any existing exceptions to monitoring rules, such as particular transaction types (e.g., intercompany transfers) or customers (e.g., “good guy” lists compiled by the FI) that may have been approved to bypass monitoring channels. To assist with calibrating and benchmarking the effectiveness of filters, existing management information system (“MIS”) data, such as performance ratios (e.g., alert to case metrics), should be reviewed to determine whether the results make sense and appear meaningful. This may involve testing above and below monitoring thresholds to observe resulting outcomes. Although third-party vendors may have been used (e.g., for system implementation or for establishing rules), testing and fine-tuning activities should be performed either in conjunction with or independent of the third party to avoid over-reliance. Further, by ensuring that testing is conducted in a consistent fashion throughout the FI, as opposed to performing in isolation, the FI is better positioned to manage risk.

Source Data and Internal Reports Relating to PSUA — The ability to produce effective and timely reports that assist in identifying PSUA (e.g., manual MIS or surveillance monitoring reports) and that adhere to U.S. and non-U.S. reporting requirements is dependent upon both the quality and completeness of the source data. If the underlying information reviewed for monitoring purposes — whether it be transaction data or KYC — is questionable, or if there are flaws in how the information flows to reporting mechanisms, the results will not be reliable. The Business Unit should possess controls for ensuring that all relevant data (e.g., the complete population of customers, accounts or transactions) are being captured and fed appropriately. The processes associated with pulling (or feeding data to automated reporting solutions) are influenced by the number of data sources involved and whether the processes are well-integrated or whether they are manual and disparate. In addition, the cleanliness of the data by way of appropriate segmentation (e.g., customer risk ratings, customer types, transaction types) is an essential component in promoting reporting efficiency. A formal process for confirming that all relevant source data is accurate, complete and timely will improve the usefulness and reliability of resulting reports.

Escalation and Referral of Activity — Policies, procedures and processes should be in place for referring PSUA from all areas of the Business Unit to the personnel or department responsible for evaluating PSUA. This includes establishing and documenting a clear and defined escalation process from the point of initial detection to the completion of the investigation. Additional channels for employees to refer PSUA privately (such as an anonymous call center) should be available and communicated in policies and procedures. If the Business Unit does not perform the investigative function itself, there is an expectation that it should maintain adequate interaction and communication with all parties involved in the process. In addition, procedures and guidance should be regularly reviewed and updated to ensure that relevant and specific examples are used to demonstrate potential escalation points.

Alert Management — Investigative units, or similar distinct groups, are often tasked with managing and researching activity identified as being potentially suspicious and determining whether they warrant further
investigation. This is often referred to as the “alert management” process. As a best practice, this process should ensure that all applicable information (e.g., criminal subpoenas, national security letters, section 314(a) requests) is effectively evaluated. Policies, procedures and processes for the timely review of, and response to, alerts used to identify unusual activities may assist in facilitating the review. To reduce risk exposure, staffing levels should be sufficient to review reports and alerts in a timely manner and the staff should possess specialized knowledge with adequate experience and research tools.

► **Investigation** — As a best practice, the process of investigating an alert and determining whether a SAR should be filed (often referred to as “case management”), should include clear decision-making and documentation standards. Designated decision makers (whether it be a committee or specific individuals) should possess sufficient authority and competence to make final SAR filing decisions. SAR documentation should be thorough and include the reason for filing (or the rationale for not filing), as well as additional considerations, such as whether to close an account as a result of continuous suspicious activity. Although the decision to file a SAR may be subjectively determined, Business Units should establish an effective investigative and SAR decision-making process that appropriately considers all available CDD and EDD information. In instances where investigative processes or SAR decisions lie within the Business Unit, additional external reviews and approvals should exist to ensure independence.

► **SAR/STR Completion and Filing** — Numerous SAR users, such as intelligence agencies, law enforcement, regulatory authorities and FinCEN, all rely on the details provided in SARs. Information provided by FIs is used to execute investigations, gather intelligence about emerging money laundering tactics, identify illegal activities and prosecute criminals. Where a decision is made to file a SAR, the quality of the SAR content is critical to the effectiveness of the suspicious activity reporting system. A well-written and detailed SAR will allow the FI to more effectively manage large volumes of filings and conduct more fruitful examinations of suspect customers or activity. Policies, procedures and processes should reflect standards and guidelines for ensuring that SARs are timely, complete and accurate, and that narratives sufficiently describe the reported activity as well as the basis for filing. This includes retaining SARs and their supporting documentation, reporting SARs to the board of directors (or a committee thereof) informing senior management and sharing SARs with head offices as necessary. By appointing dedicated and qualified individuals to review SARs through a forum that allows for discussing and sharing best practices (e.g., for addressing essential elements of information — who? what? when? where? and why?), SAR quality may be significantly uplifted. In addition, a control mechanism (such as a SAR log in the form of a simple spreadsheet or a more advanced database) to monitor, track and report on the status of all decisions (e.g., whether to file a SAR or close an account) is typically expected and can help to ensure that decisions are followed through as intended.
OFAC and Sanctions — OFAC regulations and other regional and international mandates (e.g., United Nations sanctions) include requirements to block accounts and other property or to prohibit or reject transactions with specific countries, entities and individuals as appropriate. As stated in the FFIEC manual, “All U.S. persons must comply with OFAC regulations, including all citizens and permanent resident aliens regardless of where they are located, all persons and entities within the United States, all U.S. incorporated entities and their foreign branches. In the case of certain programs, such as those regarding Cuba and North Korea, foreign subsidiaries owned or controlled by U.S. companies also must comply. Certain programs also require foreign persons in possession of U.S. origin goods to comply.”

With frequently changing and growing lists, progressively complex sanctions terms, varying guidance for how to interpret requirements and the continual rise of new and clever evasion tactics, compliance with OFAC, sanctions and embargo regulations (referred to collectively as “OFAC” herein) is an increasingly difficult responsibility that requires significant resources, ongoing attention and specialized knowledge. Even with assistance from sophisticated automated solutions and advanced technology, there is often a need to implement manual processes, such as individualized reviews for double checking alerts, confirming false positives, managing data or adjusting and testing screening mechanisms. For FI’s with a vast number of transactions and a transnational presence, the demands and potential for error are high. Due to these recognized challenges, including the intricacies of determining which requirements apply to what customers under what scenarios, OFAC controls require enhanced scrutiny and evaluation. As a minimum standard for securing a strong control environment, the Business Unit should maintain a formal and written OFAC program with necessary internal controls (screening; reporting; testing; OFAC-specific risk assessments; OFAC-specific training; dedicated resources with specialized OFAC knowledge; quality control mechanisms for ensuring appropriate actions [e.g., blocking/prohibiting] for accounts and related property). The focus of Audit’s assessment should be on the Business Unit’s ability to comply with existing laws and regulations by effectively blocking and rejecting accounts and/or payments and screening against OFAC and other government lists.

Potential considerations for assessing the strength (i.e., strong, adequate, weak) of the control include:

- **OFAC Screening and Processing** — OFAC screening controls relate broadly to the functions associated with maintaining OFAC-related lists and identifying accounts or property that may need to be blocked or transactions that may need to be prohibited or rejected, such as those involving Burma, Cuba, Iran, Sudan and/or Syria. At a minimum, formal and documented processes should be established for managing alerts, developing effective screening mechanisms (e.g., real-time screening), updating and reviewing OFAC lists and escalating alerts where appropriate. This includes, but is not limited to: checking accounts against OFAC lists prior to initial account opening (e.g., for non-customer transactions), or shortly thereafter; identifying and investigating potentially relevant transactions; managing blocked funds and accounts (e.g., status, amount, ownership details, interest, etc.); regularly testing filtering criteria for issues (e.g., misspellings and name derivations); developing and adjusting parameters as appropriate to account for known risks (e.g., false positives, truncated payment instructions, incorrectly coded or characterized transactions, “cover payments,”

---

“straight-through processing”\textsuperscript{15}; and maintaining effective processes for investigating and escalating potential matches.

In addition, as a best practice, the Business Unit may have documented analyses (e.g., formal gap analyses/reports) that reflect potential OFAC risks relating to each product/service (e.g., transactions that involve unknown third parties) and a subsequent plan for screening and monitoring for these risks. These assessments and corresponding screening processes should link to governance and risk management forums that update and educate the Business Unit on OFAC-related matters and developments (such as that of Iran turning to the automotive sector to evade sanctions legislation and attract revenue).

\textbf{OFAC Policies and Procedures} — In order to maintain an effective OFAC compliance program, OFAC-specific policies and procedures should be documented, regularly updated and tailored to the Business Unit’s risk profile, customer base, products/services, transaction activity and geographic presence. At a minimum, policies and procedures should address all aspects of OFAC compliance and controls, including customer onboarding, screening and transaction review processes; management of blocked accounts; record keeping requirements; maintaining OFAC licenses; independent testing functions; roles and responsibilities for OFAC compliance; open lines of communication; specialized training; and reporting requirements.

\textbf{OFAC Licenses} — Subject to specific provisions and clearly documented conditions, OFAC licenses allow for certain exceptions to OFAC requirements for select transactions that are deemed to be in line with U.S. policy objectives. In addition, OFAC may grant a general license that applies to a group or a category of transactions without requiring one-off approvals from OFAC. The Business Unit should ensure that an effective process is in place for verifying that these transactions comply with all terms and conditions of an OFAC-issued license prior to processing them. In addition, copies of all OFAC licenses should be collected and kept on file as appropriate.

\textbf{OFAC Reporting and Related Metrics} — In accordance with OFAC regulations, the Business Unit is required to report all blocked payments to OFAC within ten days of the occurrence and annually by September 30; once those assets or funds are blocked, they are to be placed in a blocked account. Prohibited transactions that are rejected must also be reported to OFAC within ten days of the occurrence. The Business Unit should establish effective reporting and recordkeeping processes, including maintaining complete and accurate records for all rejected transactions for a minimum of five years after the date of the transaction and for the entire period during which the property is blocked and for five years after the date the property is unblocked for blocked property or transactions. In addition to the Business Unit’s external OFAC reporting obligations, the Business Unit should have access to all internal OFAC-related metrics that exist within the FI. This might include OFAC specific data that informs customer risk (e.g., customers associated with OFAC countries/entities), product risk (e.g., products/services, such as RDC, prepay access, e-banking or correspondent accounts that present enhanced OFAC risk) and transactional risk (e.g., transactions with OFAC countries/entities). Further, this information should contain appropriate details, such as volume and dollar values.

\textsuperscript{15}According to a July 17, 2012 U.S. Senate Report, cover payments are transfers between correspondent banks in non-sanctioned jurisdictions which lack underlying payment details and can be used as a disguise for facilitating transactions with sanctioned countries or persons. Likewise, another tactic known as straight-through processing could be employed to disguise transactions as bank-to-bank transfers and circumvent OFAC filters via automated processing procedures that bypass human intervention or manual review. This was a method that evolved due to the allowance that MT202/203 SWIFT messages (or payment instructions) previously did not require identification of the underlying originator or ultimate beneficiary for bank-to-bank transactions.
Employee AML Expertise and Coverage — Despite significant advances in information technology for managing AML operations and control processes, the accountability and success over the AML program ultimately lies with the people and the respective expertise within the organization. Regulatory bodies, such as the Office of the Comptroller Currency (“OCC”), have highlighted this message by alluding to inadequate staffing as a root cause for compliance failures in several enforcement actions. Today’s environment, characterized by increased attention to compliance with AML laws and the advent of sophisticated tools and technology requiring enhanced expertise, may have accentuated the need to focus more narrowly on “the people.” In order to prevent staff-related issues and minimize the risk of human error, AML functions and responsibilities should, at a minimum, encompass an adequate number of resources, a sufficient level of aggregate AML expertise among the staff and an appropriate allocation of time to AML tasks by seasoned personnel. Staffing coverage and training should be aligned to AML responsibilities. The focus of Audit’s assessment should be on evaluating the extent to which the Business Unit’s AML functions are staffed appropriately as indicated by factors such as the number of dedicated employees, the level of expertise of assigned personnel and existing staffing plans (e.g., allocation of hours with a consideration for shared resources).

Potential considerations for assessing the strength (i.e., strong, adequate, weak) of the control include:

**AML Staffing Coverage** — In accordance with current expectation, AML-related functions should reflect an appropriate level of attention from dedicated resources commensurate with the relative degree of risk. In instances where resources are shared or partially allocated, consideration should be given to the extent of the staff’s time and availability as it relates to each AML function to ensure that staffing placement is appropriate. As a best practice, a Business Unit should be able to demonstrate that it has a staffing plan or strategy in place to account for proper AML coverage — particularly in HR areas. This includes, but is not limited to, a focus on: 

- a) total number of available resources;
- b) AML competency among those resources; and
- c) distribution of time and effort among the pool of available AML resources.

**Employee Knowledge and Capabilities** — A strong awareness of the level of competency among the staff is critical in ensuring that staff expertise and experience is appropriately aligned to existing AML functions. Formal methods for evaluating staff competency (including establishing criteria that may be representative of AML proficiency and performing some level of analysis, such as through a survey or leveraging existing employee information) is often essential for accurate quantification. Relevant indicators of expertise include:

- a) the extent of technical knowledge over the tools/systems that are required for the relevant job function(s);
- b) the level of specialized knowledge for the relevant AML area (e.g., products/services);
- c) AML-related certifications and training; and
- d) the number of years of AML-related job experience. Other useful attributes may be available in existing hiring plans or in previously documented performance expectations for the respective Business Unit.
Training and Awareness — As the expectation for skilled AML resources continues to rise, there is a growing need for training plans and curricula to be tailored, relevant, frequent and mandatory. In addition to basic AML training relating to regulatory, legal and policy requirements, staff should receive training in: a) all critical AML topics; b) Business Unit-specific information (e.g., products/services, customers, risk profiles, policies and procedures, etc.); and c) targeted and more advanced training that is relevant to roles and responsibilities. Money launderers are constantly evolving and refining their strategies. As such, training should explore recent trends — such as through case studies — and also include a focus on detecting potential risk in less apparent areas — such as in conventionally low-risk products, businesses or activity (e.g., intercompany transfers or traveler checks that may be masking the flow of funds to third parties). The intensity, scope and frequency of training should be commensurate with each employee’s job level and respective duties. Some institutions also risk-rank employees to assist with disseminating training. A diverse training and awareness program may employ multiple methods of delivery, such as “lunch and learns,” computer-based platforms, webinars, live sessions or email updates/newsletters, to offer both formalized training and proactive communication of lessons learned. Training should be continually updated and performed as necessary to incorporate current developments and changes, such as those relating to the regulatory environment or internal systems and processes. In order to ensure that training is adequate, training programs should be documented, approved and tested. Further, as part of an effective program, recordkeeping and tracking mechanisms (including reportable training metrics) can be employed to capture employee attendance and learning history.

Overall AML Infrastructure, Framework and Practices (policies, procedures and processes; management and oversight; technology and operations) — The challenge of managing and overseeing a broad range of AML activities and functions for a large and complex organization requires careful attention to the strength and design of the FI’s AML infrastructure, framework and related practices. At a minimum, these are generally influenced by, and comprised of, the following interconnected components: policies, procedures and processes; management and oversight; and technology and operations. Each area is interdependent and contributes to a collective system of checks and balances. The focus of Audit’s assessment should be on evaluating the fundamental soundness of the Business Unit’s overall AML infrastructure, framework and practices, and whether these factors are conducive to an effective and healthy AML program.

Potential considerations for assessing the strength (i.e., strong, adequate, weak) of the control include:

Management and Oversight — The AML program and associated initiatives should be commensurate with the FI’s risk profile in order to maintain efficient operations, regulatory compliance and risk management. As such, the Business Unit’s approach and tone should be aligned to the overall firm-wide governance policy; together, they should promote cooperation between AML compliance functions and the Business Unit. For a more complete picture of the FI’s overall framework, an Audit AMLRA should evaluate both firm-wide and Business Unit-specific oversight and governance practices for managing and identifying AML risk. This includes a review of: business strategy; operating controls; reporting and escalation; roles and responsibilities; resource management; responsiveness to issues; and the Business Unit’s organizational structure (including coordination with an executive and management committee or a corporate compliance function).
A formal reporting process is critical for measuring and monitoring AML risk and the effectiveness of related controls, and should be continual and comprehensive. Report data and metrics should speak to all critical areas of an AML program with appropriate detail (e.g., ongoing OFAC investigations, customer name screening matches, past due employee training, quantity of aging alerts, monthly account closures, case management escalations, weekly SAR filings, open enforcement requests, etc.) and be reviewed with the business lines, operations department, compliance department and senior executives as appropriate. An effective reporting vehicle will allow the Business Unit to identify and measure risk as well as subsequent risk trends (e.g., whether risk is increasing or decreasing). Roles and responsibilities should be documented, transparent and defined. This includes indicating accountability (and possibly linking to performance evaluation) as well as designating specific individuals to coordinate and manage day-to-day oversight over the AML program and the Business Unit’s AML activities; where this is performed by an independent compliance function, such as a governance committee, there should be a formal and open line of communication between the business and compliance. In all cases, the Business Unit should possess awareness of relevant AML issues, such as through formal representation at important firm-wide AML meetings and forums.

Personnel in management and oversight roles should stay abreast of external AML-related events and topics and have access to necessary resources (e.g., employees, information, tools) and the ability to escalate issues promptly. In addition, self-assessment and compliance testing functions should be ongoing and allow for timely identification and monitoring of issues and any corrective actions that ensue — including a formalized process for documenting, communicating and responding to results. Compliance testing in particular should reflect independence from the business, sufficient transaction testing, tailored testing procedures and work papers that demonstrate a connection between the compliance department’s risk assessment results and respective action plans.

**Policies, Procedures and Processes** — As part of developing a comprehensive AML program, FIs are expected to develop policies, procedures and processes to monitor and mitigate AML risks relative to regulatory expectations, compliance requirements and business-specific considerations. Where appropriate, policies, procedures and processes should address the unique attributes of the Business Unit, including size, structure, customer base and product usage. Although the sophistication of the internal control environment may vary to align with risk, each Business Unit should, at a minimum, have written policies and procedures, quality management functions and risk assessment processes.

Policies (the “what”) and procedures (the “how”) should be documented, approved (e.g., by board of directors, senior management, AML governance committees), comprehensive, consistent with best practices and regularly updated to address — and remain current with — critical AML areas (e.g., KYC, suspicious/unusual activity, OFAC and sanctions, training). Exception processes (such as for deviating from global AML policies) should be clearly documented with necessary details (e.g., the approvals that need to be obtained). In general, policy and procedural documents that apply on a global and firm-wide basis (and that describe processes in a thorough manner that can be easily understood) are more likely to promote consistency and quality. This might involve the inclusion of examples, illustrations, a strong flow, references and links to helpful resources and contact details for additional information. If policies and procedures do not provide the appropriate level of granularity, there should be accompanying guidance to address how they should be applied.

A risk assessment process should be in place to evaluate the Business Unit’s inherent risks (e.g., clients, products, transactions, geography) and control environment factors (e.g., KYC, screening, training, reporting,
monitoring, etc.) at least every twelve to eighteen months (preferably annually with interim assessment exercises as appropriate, such as for the introduction of new products/services or business changes). The results of the Business Unit’s risk assessment should be consistent with its risk appetite and its respective business practices (e.g., transaction monitoring scenarios should be aligned to HR areas and unique risks noted in the assessment). As a complementary measure, the Business Unit may want to formalize a process for documenting, evaluating and adjusting its risk appetite. Quality management functions for ensuring quality, consistency and adherence to the Business Unit’s policies, procedures and processes should be documented, approved and embedded in day-to-day operations where appropriate. In addition, specific limitations may be appropriate for particular customer or account types (e.g., minimum asset sizes for third-party payment processors to open accounts; restrictions for MSBs to offer no more than one product line, such as check cashing; funds transfer limits for payable-through-accounts; yearly limits on the number of international wires that can be initiated from corporate checking accounts). In instances where outside providers (e.g., vendors or consultants) are used to assist with policies, procedures or processes, the FI maintains accountability and, as such, is responsible for demonstrating tight oversight, such as through due diligence, reporting lines, sample testing, review and approval of its work and stringent documentation requirements.

**Operations and Technology** — The nature of a Business Unit’s operations and its associated technological capacity are strong indicators of whether a Business Unit is capable of sustaining an effective and well-balanced AML program that can defend against everyday AML risks and adhere to applicable regulations and responsibilities. FIs are responsible for ensuring that AML functions are well-connected, that events (e.g., results from FI systems or processes) are viewed holistically, and that proper feedback loops are in place across the AML program (e.g., that KYC information informs the nature of transaction monitoring and that transaction monitoring results feed back into the KYC processes to inform the level and type of information needed). In addition to reinforcing the flow between control environment components, the FI and Business Unit should ensure that operational processes and automated solutions are effective and working as intended for all relevant risk areas. Routine and standard AML operations and functions (e.g., currency transaction reporting, recordkeeping activities, data management, monetary logs, Section 314(b) information sharing, compliance with OFAC and sanctions reporting) should address regulatory requirements and align to the FI’s global AML policy. Documented procedures, adequate staffing and periodic testing functions with formalized results may be additional signs of a strong operating environment. Technology-driven mechanisms should have the flexibility to adapt to changes and the capacity to support all required business activities and controls, such as those relating to reporting, data mining, record retention, business recovery, information security and monitoring. Data management and analytics practices relating to AML information should be consistent across the business and allow for appropriate accessibility, interpretation and storage.

A large number of technology platforms or systems that are disconnected from each other may lead to operational challenges and inconsistencies (e.g., discrepant retrieval and analysis of customer information). A portion of this burden may be minimized through a process that looks at whether the same reference codes for customer, product and transaction types are being applied (e.g., consistent labeling of PEPs) or reconciled (e.g., different codes are identified and assigned a common identifier) or whether the same source data is being referenced for similar activities or reports (e.g., onboarding of PEPs across the Business Unit). Further, the presence of numerous or large-scale projects (e.g., “lookbacks,” KYC “remediations,” procedural updates) or changes (e.g., moving to a new monitoring system, merging of business lines) may present vulnerabilities in the control environment due to resource exhaustion or risks associated with employing change, such as learning new systems, managing data or errors that go undetected.
Central units may own particular controls, but the respective business area owns the risk. As part of a comprehensive risk assessment, each Business Unit should possess an understanding of the risks and controls that affect its business — independent of whether these controls are either partially or fully owned by a separate Business Unit. In instances where an AML service is provided centrally (e.g., customer onboarding, screening, training, monitoring, investigating), it is important for Audit to: 1. evaluate the Business Unit’s understanding over the central unit’s processes, control effectiveness and potential risk impact of a control failure; and 2. determine whether the Business Unit has supplemental controls in place to either manage the risk on its own or to minimize reliance on the central function.

The impact of a control failure within a central function may vary depending on: a) a Business Unit’s underlying susceptibility to the risk being mitigated (i.e., a Business Unit with a low-risk customer base may be less impacted by a KYC control failure than a Business Unit with a high-risk customer base); or b) whether the Business Unit owns additional controls (i.e., a Business Unit that maintains Quality Assurance [“QA”] processes over a central unit’s activities and performs periodic sample testing may be less susceptible than a Business Unit that is fully reliant and detached from the control processes).

THE SUPPORT FRAMEWORK: Investing in Audit’s risk assessment process

In addition to providing auditors with guidance by defining and describing risk and control environment factors and supplying helpful considerations, a strong support framework involves adequate resourcing and education; identifying and addressing common challenges; and promoting healthy practices. This investment in Audit’s risk assessment process can provide valuable dividends in the form of execution efficiencies, better quality results and potentially reduced exposure to adverse regulatory feedback. A few critical elements in this area include:

Subject Matter Expertise and Keeping Assessments Current

The identification and analysis of AML risk can be complex. An accurate assessment of AML risk often requires specialized knowledge in AML as well as a strong understanding over the Business Unit (e.g., activities, products/services, customers, geographical presence) and any region-specific considerations (e.g., laws, regulations, country risk) that may be applicable. In a perfect world, the auditor completing the assessment would be knowledgeable in all three areas; however, this may not always be feasible. By establishing a network of AML subject matter experts and designated individuals or groups to represent each region and business area, the auditor has access to a valuable pool of information and is better positioned to identify and assess unique AML risks. At the very least, each risk assessment should involve input and oversight from individuals with the requisite AML credentials, experience, training and subject matter expertise prior to completion.

Keep in mind that: Assessing and documenting potential risks is an ongoing process that requires a continuous flow of information between those with visibility and accountability over AML matters and those who are responsible for Audit’s risk assessments. As such, risk assessments should be revisited as necessary or periodically (e.g., quarterly or semi-annually) to reflect relevant current events, such as internal developments (e.g., mergers, acquisitions, divestitures, technology/systems enhancements, new products/services, emerging risks/issues and other changes in business activities) or external developments (e.g. regulations, industry expectations). One method to assist with this includes establishing a culture of communication and outreach, such as a forum for sharing information and discussing recent events among business representatives, regional representatives, AML subject matter experts and Audit members.
Continual Training and Guidance Specific to Risk Assessments

The development and distribution of formal training, policies/procedures and equivalent guidance promotes consistency and enhances the audit department’s ability to assess AML risk. At a minimum, documented and approved materials should describe the risk assessment process, the risk scoring/rating methodology, documentation standards, roles and responsibilities and the identification and analysis of AML risk. For best results, materials should be easily accessible and reviewed for clarity, relevance and completeness.

Keep in mind that: For additional support, a separate function or role can be tasked with providing continual feedback and guidance, such as through the use of case studies, live examples and/or periodic group discussions. This role may supplement, or include, a formal quality control ("QC") process for reviewing Audit’s completed risk assessments and providing helpful feedback. By gathering and reviewing current assessments through QC processes, pilot testing, sampling methods or equivalent mechanisms, the audit department can compile and compare results, which can then be used to create training tools, such as "lessons learned." Relevant and carefully crafted guidance materials (as well as the delivery channels) can be instrumental in addressing frequently asked questions, maintaining consistency, instilling best practices and educating those responsible for completing risk assessments.

Supporting Data

To facilitate the task of obtaining supporting data and information for completing the risk assessment, a formal firm-wide process can be developed prior to the launch of the risk assessment. This might include developing a strategy for collecting information, understanding where the data resides, ascertaining the quality of the data, assigning one or more project managers/ coordinators to oversee the process, identifying common data that can be shared across Business Units, establishing a relationship with personnel that can provide information and designating a central location for storing and accessing materials. Due to the extensive labor involved with this exercise, it is helpful to view and manage this process as a standalone project.

As part of establishing critical relationships and maintaining a strong support network, the audit department should engage the business leadership from each line of business as well as the technology department to assist with accessing and procuring data. The use of a tool (e.g., a document list) that indicates potentially helpful sources as well as the likelihood of obtaining them and the particular areas where they are most useful, may further minimize the collection burden. This should be accompanied by a tracking mechanism for capturing and reporting on requested information through the process. Although particular metrics and reports may be specific to a Business Unit, there may be common sources of information that are easier to obtain and that serve useful across multiple Business Units. (Examples include regulatory examination feedback, audit findings, compliance testing results, self-assessments performed by the business, prior risk assessments, meeting minutes/agendas, management reports, process flow charts, job-aids and related manuals, firm-wide policies and procedures, etc.). For best results, individuals with working knowledge over the FI’s source data and internal systems should be leveraged as much as possible.

Keep in mind that: The use of supporting data is influential (and increasingly expected) in demonstrating how risk decisions and conclusions were derived. Quantitative information (such as transaction volumes and types and customer population demographics by risk category and location) should be used and documented as much as possible when making inferences. However, careful consideration should be applied when determining how and when supporting information should be leveraged and what a deficit of such information may suggest for the risk rating. A business’ inability to provide key data may be reflective of a control failure, particularly if the information is necessary for day-to-day operations or is expected by firm policy.
Direction for Crafting a Strong Narrative

A clear, concise and consistent narrative is critical for evidencing rating decisions and articulating potential risks. Although the ability to effectively communicate and describe one’s findings through a written analysis may seem more like an art form than an exact science, there are particular strategies that can be leveraged to enhance the overall assessment. These include, but are not limited to: starting with an introductory description of the Business Unit (e.g., general overview of what the Business Unit does and the AML-related functions or services that it provides or supports either directly or indirectly); linking to, and referencing, supporting sources of information where possible (e.g., particular documents, data, reports, contacts); representing quantitative support in the context of the Business Unit (e.g., explaining what the numbers mean and the respective impact); avoiding information overload (e.g., using comments that are relevant to the assessment and focus on the single most important factors that substantiate the ratings); managing the flow and organization of responses (e.g., bundling comments in a manner that clearly aligns to, and addresses, each risk and control factor); indicating directional risk trends; and including a brief conclusion that summarizes the rationale for the final Business Unit risk rating.

Keep in mind that: Third parties and those who are unfamiliar with the Business Unit should be able to read through the narrative and reach the same conclusions as the auditor that conducted the assessment. For this reason, the assessment should be crafted as a self-sufficient evaluation of the Business Unit with adequate detail.

INTERPRETING AND USING RESULTS: The audit plan and beyond

<table>
<thead>
<tr>
<th>Example - for illustration purposes only</th>
<th>INHERENT RISKS</th>
<th>CONTROL ENVIRONMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Unit A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Unit B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Unit C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Unit D</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Subsequent to completing Audit’s risk assessment process, the audit department has access to a high-quality toolbox with which to corroborate results, assemble a comprehensive risk-based plan and illustrate a bird’s eye view of AML risk within the enterprise. Prior to preparing the audit plan, the resulting ratings and scores for each Business Unit (which may be developed in conjunction with the firm’s existing risk scoring and rating model) can be used to drive a targeted review of select risk assessments based on factors such as whether ratings appear reasonable, whether inconsistencies are present or whether there are outright conflicts with current audit findings and/or perception. After evaluating AMLRA results and obtaining a reasonable level of comfort as to the data quality, Audit will possess a valuable set of data points that can be used to compile an audit plan that evaluates risk from a variety of angles, such as overall risk, changes in risks, business area, geography, central functions/process or prior coverage.

With proper analysis, AMLRA data can be dissected and stratified to assist in ranking and prioritizing potential audits in relation to each other. If for instance, two Business Units in a similar area appear to present similar risk, the decision to include one Business Unit in the plan over the other may be based on whether one of the Business Units has recent audit coverage, or whether another audit in the plan covers the same region as one of the two.
AMLRA output can also be used to identify relevant trends or themes that may warrant further review. If multiple Business Units have cited a common weakness or risk within their AMLRA (e.g., a specific process, function, product or customer type) this may call for an audit that looks horizontally across the organization at this particular element.

In addition to assisting with audit planning, the results of the AMLRA enable top-down views within the organization and provide periodic snapshots of AML risk, which allow for meaningful year-over-year comparisons. Audit can use these views to identify whether AMLRA results deviate from current expectation. Where variances exist, the available data set can then be further examined for reasonable explanations. If for instance, an identified pattern indicates that risk relating to OFAC screening has decreased since the prior period across five Business Units — all of which have shifted to using a specialized screening hub that was recently launched — this might suggest that the hub is effective. Alternatively, if a variance cannot be explained, this might warrant escalation to the business and further exploration.

**TAKEAWAY: The risk assessment “design” can better equip Audit**

Through its role as the eyes and ears of the enterprise, the audit department is uniquely positioned to independently identify AML risks and trends, to inspect the control environment, to test the sustainability of the AML program, to assist the business functions in maintaining effective risk management behaviors and to intervene as necessary to ensure that potentially material issues are recognized, understood and addressed. As such, Audit is a vital player and an essential line of defense in protecting the FI and ensuring compliance with regulatory matters and safe business practices. In accordance with this responsibility, Audit’s risk assessment process is an integral component in evaluating the nature and extent of AML risk and supporting Audit’s planning decisions. Although there is currently no specific model, method or format for framing the risk assessment, the design of an AMLRA tool, including the supporting framework, has a significant impact on the resulting output that will be used to drive Audit’s testing activities.

Regardless of whether the tool is web-based or designed in MS Word, MS Excel or through a proprietary vendor, the development of the AMLRA tool should encompass core AML principles and criteria that can be used as a benchmark for guiding the assessment process without endorsing a checklist-style approach. This can be achieved through a structure that points auditors towards relevant considerations, yet facilitates thoughtful analysis and supported decision making within the assessment. A multifaceted design that is comprehensive, dynamic and sustainable in nature is a valuable control that helps with producing meaningful results that can be used to direct Audit and its testing focus. This includes dedicating sufficient resources to the risk assessment process and promoting an emphasis on detailed commentary, documenting whether risk is increasing/decreasing in particular areas, demonstrating the rationale behind rating decisions and evidencing conclusions via supporting data.
Although the act of enhancing the design of an Audit risk assessment tool may sound like a small step, the effect may be substantial if it leads to a more accurate, substantive and reliable audit planning and testing program. As of now, the relationship between regulator and auditor may lean more toward that of examiner and examinee; however, by instilling the proper confidence, this relationship may shift to a partnership — one which, between the regulator’s wealth of aggregate industry knowledge and the auditor’s “inside” operational and technical knowledge, is a much more powerful force for *Combating Money Laundering and Terrorist Financing.*
How to Build an Audit Risk Assessment Tool to Combat Money Laundering and Terrorist Financing

APPENDICES

A - Overview of considerations

INHERENT RISK CONSIDERATIONS

<table>
<thead>
<tr>
<th>Customers</th>
<th>Products and Services</th>
<th>Transaction Activity</th>
<th>Geographic Presence</th>
</tr>
</thead>
<tbody>
<tr>
<td>HR Customer Types</td>
<td>HR Products and Services</td>
<td>Activity Involving HR Product/Services</td>
<td>Customers in HR Locations</td>
</tr>
<tr>
<td>Duration of Relationship</td>
<td>New Products and Services</td>
<td>International Activity</td>
<td>Physical Presence in HR Locations</td>
</tr>
<tr>
<td>Closed/Blocked Accounts</td>
<td>Business/Sales from HR Products and Services</td>
<td>Transactions Involving Indirect Parties</td>
<td>Transactional Activity with HR Locations</td>
</tr>
<tr>
<td>Number and Nature of Accounts</td>
<td>Risk Tolerance and Business Strategies</td>
<td>Reportable Transaction Activity</td>
<td></td>
</tr>
</tbody>
</table>

CONTROL ENVIRONMENT CONSIDERATIONS

<table>
<thead>
<tr>
<th>KYC</th>
<th>Suspicous and/or Unusual Activity</th>
<th>OFAC and Sanctions</th>
<th>Employee AML Expertise and Coverage</th>
<th>Overall AML Infrastructure, Framework and Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exceptions or Waivers</td>
<td>Detection and Monitoring</td>
<td>OFAC Screening and Processing</td>
<td>AML Staffing Coverage</td>
<td>Management and Oversight</td>
</tr>
<tr>
<td>Reliance</td>
<td>Source Data and Internal Reports Relating to PSUA</td>
<td>OFAC Policies and Procedures</td>
<td>Employee Knowledge and Capabilities</td>
<td>Policies, Procedures and Processes</td>
</tr>
<tr>
<td>Completeness of Customer Information</td>
<td>Escalation and Referral of Activity</td>
<td>OFAC Licenses</td>
<td>Training and Awareness</td>
<td>Operations and Technology</td>
</tr>
<tr>
<td>Renewals, Updates and Periodic Reviews</td>
<td>Alert Management</td>
<td>OFAC Reporting and Related Metrics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer Name Screening</td>
<td>Investigation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAR/STR Completion and Filing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

APPENDICES

A - Overview of considerations
B - Examples of considerations

Inherent Risks — Examples of Higher Risks

Customers

HR Customer Types
The Business Unit reflects a significant number of accountholders categorized as HR per the FI's pre-existing customer risk rating model.

Duration of Relationship
The Business Unit reflects a significant number of accounts (those representative of establishing a new customer relationship) that have been opened within the past twelve months.

Closed/Blocked Accounts
The Business Unit reflects a significant number of customer accounts or relationships that have been closed or blocked at the direction of the FI.

Number and Nature of Accounts
The Business Unit reflects a significant number of customers with open (e.g., active and/or dormant) accounts in, or having access to, other Business Units within the FI.

Products and Services

HR Products and Services
The Business Unit offers a significant number of HR products/services or reflects a significant number of customers that use HR products/services.

New Products and Services
The Business Unit offers a significant number of recently introduced products/services or reflects a significant number of customers that use these products/services.

Degree of Business/Sales Generated from HR Products and Services
The Business Unit’s total business portfolio reflects a significant dollar amount of revenue that is attributed to the sale of new products/services.

Risk Tolerance and Business Strategies
The Business Unit has self-evaluated (or has indicated elsewhere) a high risk tolerance or the Business Unit has requested to forego firm-wide AML requirements or processes despite known risks.

Transaction Activity

Activity Involving HR Products/Services
The Business Unit reflects a significantly high volume or dollar amount of activity involving high risk products/services.

International Activity
The Business Unit reflects a significantly high volume or dollar value of international activity.
Transactions Involving Indirect Parties
The Business Unit reflects a significantly high number of customers and/or accounts with the capability to conduct transactions with (or on behalf of) non-FI customers through the FI.

Reportable Transaction Activity
The Business Unit reflects a significantly high number of customers with transaction activity reporting.

Geographic Presence
Customers in HR Locations
The Business Unit reflects a significant number of customers with known addresses in HR locations.

Physical Presence in HR Locations
The Business Unit has an operating branch in a significant number of HR locations.

Transactional Activity with HR Locations
The Business Unit reflects a significant number of customers with accounts that exhibit transactions with HR locations.

Control Environment and Risk Mitigants — Examples of Control Weaknesses

KYC
Exceptions or Waivers
The Business Unit reflects a significant number of exceptions or waivers to internal KYC policies, procedures or standards.

Reliance
The Business Unit reflects reliance on other parties for KYC functions and does not receive metrics/status reporting, does not own controls for monitoring or managing the reliance, does not reflect accountability or does not demonstrate an understanding over the process and potential risk impact.

Completeness of Customer Information
The Business Unit reflects a significant number of active accounts with missing or incomplete KYC information.

Renewals, Updates and Periodic Reviews
The Business Unit reflects a significant number of accounts that have not been renewed or updated in accordance with its renewal cycle.

Customer Name Screening
The Business Unit reflects deficiencies in identifying name matches; there are inconsistencies in screening practices or there is poor interaction between Business Unit and central function.

Potentially Suspicious and/or Unusual Activity
Detection and Monitoring
The Business Unit is not appropriately equipped to identify and monitor PSUA (e.g., lack of training, procedures or access to reports) or the Business Unit reflects frequently identified system deficiencies and issues, such as parameters that are not working as intended or failures to effectively detect deviations between expected and actual activity.
Source Data and Internal Reports Relating to PSUA
The Business Unit does not have an approval process to ensure that data is accurate, complete and timely, or the reports being produced contain errors and/or related deficiencies.

Escalation and Referral of Activity
The Business Unit cannot produce evidence of a documented and defined escalation and referral process.

Alert Management
The Business Unit reflects a large or increasing number of open alerts, or decisions on whether to further investigate alerts are not clearly documented or approved.

Investigation
The Business Unit does not have procedures that detail documentation standards or describe the process for closing of accounts due to continuous suspicious activity.

SAR/STR Completion and Filing
The Business Unit has a significant number of SARs that have been corrected, reversed or identified as being incomplete, weak or outstanding.

OFAC and Sanctions
OFAC Screening and Processing
The Business Unit contains a significant number of alerts that have not yet been reviewed; there are a significant number of manual or interim processes in place; or transactions flagged as requiring specific actions (e.g., blocking) are not compliant with the appropriate measures.

OFAC Policies and Procedures
The Business Unit does not adequately update policies and procedures to account for continual OFAC-related developments; does not maintain written, comprehensive and approved policies and procedures for all critical OFAC program areas; and does not exhibit OFAC practices that are consistent with those documented in and required by internal OFAC policies and procedures.

OFAC Licenses
The Business Unit exhibits ineffective processes or procedures for verifying OFAC-issued licenses or does not adequately retain copies of licenses where appropriate.

OFAC Reporting and Related Metrics
The Business Unit does not report all blocked and/or prohibited transactions to OFAC on a timely basis; records are not full and accurate where applicable; or OFAC management reports reflect deficiencies in content, distribution or frequency.
Employee AML Expertise and Coverage

AML Staffing Coverage
The Business Unit does not reflect a sufficient level of competent staff among critical AML functions or does not conduct AML specific capacity planning or equivalent staffing analyses.

Employee Knowledge and Capabilities
The Business Unit reflects a low level of staff with advanced or adequate AML competencies relative to the required AML function.

Training and Awareness
The Business Unit’s training content is not accurate, relevant or complete; employees are not completing required trainings; attendance is not being tracked; or training frequency is inadequate.

Overall AML Infrastructure, Framework and Practices

Management and Oversight
The Business Unit has inconsistent management reports, reflects inaccuracies in metrics, does not report on critical AML matters (e.g., number of open accounts associated with PEPs) or has testing functions that are infrequent and ineffective in identifying issues, including those known to Audit.

Policies, Procedures and Processes
The Business Unit’s risk rating methodologies for its risk assessments are undefined and rating decisions do not reflect adequate support; or quality management processes are inconsistent, undocumented or deficient for critical areas, such as for SAR filing or customer on-boarding.

Operations and Technology
The Business Unit reflects deficiencies in executing day-to-day operations, such as maintaining adequate monetary logs or reporting on currency transactions; the technological environment is incapable of monitoring the volume and complexity of customer transactions; there is lack of management over third-party processing; or methods for interpreting and defining data are inconsistent.
C - References

   http://www.bis.org/publ/bcbs230.htm
   http://www.nytimes.com/2013/06/04/world/middleeast/us-adds-to-its-list-of-sanctions-against-iran.html?_r=0
    http://www.fas.org/sgp/crs/mideast/RS20871.pdf


www2.acams.org/webinars


http://www.coso.org/ic.htm


http://www.issai.org/media/13341/intosai_gov_9130_e.pdf


www2.acams.org/webinars


http://www.fdic.gov/regulations/examinations/supervisory/insights/siwin09/From_Examiners_Desk.html


Enforcement Actions


3. United States of America before the Board of Governors of the Federal Reserve System. Consent Order. #13-004-B-HC.


D - Helpful resources for rating and scoring

ERM Risk Assessment in Practice (2012)

Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies - SR 95-51 (SUP) November 14, 1995

Federal Reserve System Framework for Risk-Focused Supervision of Large Complex Institutions

E - Acronyms and terms used throughout this paper

ACAMS — Association of Anti-Money Laundering Specialists.

Account (term) — A formal banking relationship established to provide or engage in services, dealings or other financial transactions including a deposit account, a transaction or asset account, a credit account or other extension of credit. Account also includes a relationship established to provide a safety deposit box or other safekeeping services, or cash management, custodian and trust services.

ACH — automated clearing house.

AML — anti-money laundering.

AML (term) — Encompasses the Bank Secrecy Act, anti-money laundering, Office of Foreign Assets Control and sanctions.

AMLRRA — AML risk assessment.

Audit (term) — The internal audit department.

BSA — Bank Secrecy Act.

Business Unit (term) — An auditable business area, control function/utility and/or lines of business.

CDD — customer due diligence.

CIP — customer identification program.

COSO — Committee of Sponsoring Organizations.

CTR — currency transaction reports.

Customer (term) — A "person" (an individual, a corporation, partnership, a trust, an estate or any other entity recognized as a legal person) who opens a new account, an individual who opens a new account for another individual who lacks legal capacity, and an individual who opens a new account for an entity that is not a legal person (e.g., a civic club). A customer does not include a person who does not receive banking services, such as a person whose loan application is denied.

EDD — enhanced due diligence.

How to Build an Audit Risk Assessment Tool to Combat Money Laundering and Terrorist Financing

FDIC — Federal Deposit Insurance Company.
FFIEC — Federal Financial Institutions Examination Council.
FI — Financial institution.
FinCEN — Financial Crimes Enforcement Network.
HIDTA — high-intensity drug trafficking area.
HIFCA — high-intensity financial crime area.
HR — high-risk.
INTOSAI — International Organization of Supreme Audit Institutions.
KYC — Know Your Customer.
LOB — lines of business.
MIS — management information system.
MRA — matter requiring attention.
OCC — Office of the Comptroller Currency.
OFAC — Office of Foreign Assets Control.
OFC — offshore financial center.
PEPS — politically exposed persons.
PSUA — potentially suspicious and/or unusual activity.
QA — quality assurance.
QC — quality control.
RCCs — remotely created checks.
RDC — remote deposit capture.
Risk Appetite (term) — The amount of risk on a broad level that an entity is willing to accept in seeking to achieve its objectives.
SAR — suspicious activity report.
SDN — specially designated nationals.
STR — suspicious transactions report.
Tool (term) — The mechanism (such as a basic template or system) used to organize, record, assess and rate AML risks. A tool can be a sophisticated system or a simple spreadsheet, as well as any accompanying guidance.
F - About the author

Jonathan Estreich is currently a vice president within the internal audit department at JPMorgan Chase. With over eight years of experience working with financial services firms such as Deloitte Financial Advisory Services LLP and UBS Investment Bank, Mr. Estreich specializes in providing anti-money laundering and counter-terrorist financing services with a focus on AML policies, procedures and internal controls, including those relating to transaction monitoring, Know Your Customer initiatives, customer due diligence and risk assessments. By servicing many different financial institutions within the banking sector in multiple capacities, he has accumulated a broad range of industry knowledge and expertise in diverse areas such as global AML compliance and Office of Foreign Assets Control as well as in working with complex product and customer types. He has had considerable involvement in leading, managing and advising on BSA/AML-related matters, including authoring several works with Thomson Reuters Complinet, ACAMS Today, InsideCounsel and Corporate Compliance Insights.

Professional credentials include:

Certified Fraud Examiner (CFE)
Certified Anti-Money Laundering Specialist (CAMS)
Advanced Anti-Money Laundering Audit designation (CAMS-Audit)
Certified Associate in Project Management (CAPM)

Related works by the author

2. Understanding recent developments in prepaid access: Considerations for deterring money laundering, ACAMS Today, (March 2012).
4. CISADA Section 104(e): A glance into the final rule’s counter terrorist financing requirements and challenges for U.S. Financial Institutions, Corporate Compliance Insights, (October 2012).