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

REFERENCE GUIDE

Jonathan Estreich
December 2014

ACAMS® Advancing Financial Crime Professionals Worldwide
The author is not necessarily representing the views or opinions of JPMorgan Chase or ACAMS. This document serves as a supplemental resource to the whitepaper published in December of 2013: How to Build an Audit Risk Assessment Tool to Combat Money Laundering and Terrorist Financing.
Objective
To provide specific considerations for how a financial institution’s internal audit department can “design” a firm-wide AML risk assessment tool that:

- **Improves the auditor's ability** to identify relevant AML risks
- **Sets the foundation** for thoughtful and supported risk determinations
- **Produces results** that can assist in the development of an audit plan that satisfies regulatory expectations

Introduction
“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.”
Key Points

1. Regulatory expectations are high and the auditor’s role is evolving

Regulators are emphasizing the importance of independent testing and the role of the AML auditor in helping to manage risk and sustain an operational AML program.

“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.”

Includes a review of the FI’s risk assessment for reasonableness given the FI’s risk profile:

- Customers
- Products and Services
- Transaction Activity
- Geographic Presence

Additional focus on:
- Risk tolerance
- The level of assurance
- The depth and precision of controls
- The nature of substantive testing
- The degree of credible challenge

Regulatory Orders (2012, 2013)
- Inadequate CDD and EDD practices
- Incomplete identification of high-risk customers
- Insufficient policies, procedures and training
- Failures in monitoring and identifying suspicious activity
- Poor suspicious activity reporting and filing practices
- Ineffective independent testing and audit functions

2. The audit plan indicates to regulators whether Audit is on track

3. Audit’s risk assessment process drives the audit plan

4. There “is” a difference between an Audit AMLRA and other AML risk assessments
2. The audit plan indicates to regulators whether Audit is on track

“Audit is responsible for assembling an audit plan that demonstrates its organization’s knowledge of its Business Units and an understanding of the business’ associated risks.”

The Audit Plan:
- Primary roadmap for AML testing activities
- If the plan is lacking, the FI may be exposed
- Should, at a minimum, focus on the highest-risk areas

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.

A successful risk assessment should:
- Result in a detailed risk profile for each Business Unit
- Demonstrate the rationale and inform decisions for including or excluding a specific audit area in the plan

3. Audit’s risk assessment process drives the audit plan

Audit is expected to select audits using a risk-based approach that provides a reasonable belief that critical risks are identified and assigned adequate testing coverage in a timely fashion.

“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 process of building the audit plan should involve consideration of:
- Existing or Prior Audit Coverage
- Unique Business Risks
- Pre-existing issues
- Severity of AML risk factors

Adapted from: The SAR Activity Review—Trends, Tips and Issues (Issue 16), (October, 2009).
4. There “is” a difference between an Audit AMLRA and other AMLRAs

Differences between risk assessment tools do exist, and these may be attributed to who the tool is designed for and how the results will ultimately be used.

“It is reasonable for Audit to reflect a combined approach of independently deriving some pieces of information while leveraging other pieces—granted a reasonable level of comfort.”

**AUDIT AMLRA**

IDENTIFY AND ASSESS RISK WITH THE PURPOSE OF:

1. Pinpointing areas warranting immediate escalation
2. Pinpointing areas warranting further substantiation and testing

Usually completed by an auditor or other audit department designee

**Key Points**

An effective Audit AMLRA should assist with audit decisions relating to:

- Whether the FI’s risk assessment processes are effective
- What Business Units should be audited
- What AML components within a Business Unit may warrant testing coverage
- The frequency for which a Business Unit may need to be tested
- Prioritization and timing of audit coverage across Business Units
- Potential resourcing demands for conducting the resulting audits
Developing The Tool

1. Overview
A strong AMLRA design leads, directs and guides the auditor’s focus and helps the auditor to successfully assess risk while avoiding generalizations.

Commonly cited risk assessment weaknesses:
- Assessments were not performed and/or not evidenced through documentation
- Assessments did not include all lines of business or entities
- Assessments did not consider all major risk categories
- There was a lack of methodology for assigning risk ratings/levels
- Policies and procedures were not commensurate with the institution’s risk profile

Adapted from: “Spotlight on Large Institutions: Conducting Enterprise-Wide AML Risk Assessments that Go Beyond the Expectations of Examiners and Senior Management,” ACAMS; June 26, 2013

An AMLRA tool should be conducive to:
- Identification of Risk
- Quantification of Risk
- Assessment of Risk
- Documentation of the Level of Risk

“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.”

1. Overview
2. Basic Factors
3. Risk Factors
4. Control Factors
5. General
2. Basic Factors
The development of a robust risk assessment model is largely dependent upon the individual elements that are chosen as the Risk and Control Environment Factors to be assessed and evaluated.

“FIs are expected to establish a control environment that minimizes and—where possible—safeguards against AML risks.”

“[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.”

3. Risk Factors
The process of identifying and assessing the degree of inherent risk will help to quantify the extent of residual risk, which in turn can inform audit planning decisions.

Inherent Risk Considerations (Example) — CUSTOMERS

- **HR Customer Types**
The Business Unit reflects a significant number of account holders 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.

“The focus of Audit’s assessment should be on identifying the extent to which the Business Unit’s customer population reflects high-risk characteristics such as those outlined here.”
Guidance & Training Tips (Example)

“How magnitude provides perspective; be sure to consider context when assessing and documenting statistics and other metrics.”

- 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.
- 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.

“You might not own customers or products, but look deeper for potential AML risk.”

- For areas such as technology 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.
- Consider transactional activity (e.g., with vendors or counterparties) and think holistically about the Business Unit’s “potential” (e.g., in the absence controls) to influence AML Risk, such as whether the Business Unit affects risk in other business areas within the FI.

3. Control Factors
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.

CONTROL ENVIRONMENT CONSIDERATIONS

<table>
<thead>
<tr>
<th>KYC</th>
<th>Suspicious 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 PSU</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></td>
<td>SAR/STR Completion and Filing</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Control Environment Considerations (Example) — KYC

- **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.

- **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.

“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.”
“Central units may own particular controls, but the respective business area owns the risk.”

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.

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.

“While business provided data should be tested, it may not always be feasible to substantiate and independently validate all pieces of information as part of the Audit AMLRA process.”

At the risk assessment stage, there may be instances where it is reasonable for Audit to allow for some level of reliance on existing information when drawing conclusions.

Audit should have a reasonable level of comfort that the leveraged information is accurate and/or reliable (such as through previous validation exercises).
How to Build an Audit Risk Assessment Tool to Combat Money Laundering and Terrorist Financing

**Subject Matter Expertise**
- Specialized knowledge in AML
- Strong understanding over the Business Unit
- Region-specific familiarity

“Each assessment should involve input and oversight from individuals with the requisite AML credentials, experience, training and subject matter expertise.”

**Continual Training and Guidance Specific to Risk Assessments**
- Risk assessment process
- Risk scoring/rating methodology
- Documentation standards
- Roles and responsibilities
- Identification and analysis of AML risk

“The development and distribution of formal training, policies/procedures and equivalent guidance promotes consistency and enhances Audit’s ability to assess AML risk.”

**Supporting Data**
- Develop strategy for collecting information
- Understand where the data resides
- Ascertain the quality of the data
- Assign project managers/coordinators
- Designate a central location for storage/access

“Due to the extensive labor involved with obtaining data, it is helpful to view and manage this process as a standalone project and formalize as much as possible.”

**Direction for Crafting a Strong Narrative**
- Including an introductory description of the BU
- Referencing supporting sources of information
- Representing quantitative support in context of the BU
- Avoiding information overload
- Managing the flow and organization of responses
- Indicating directional risk trends

“A clear, concise and consistent narrative is critical for evidencing rating decisions and articulating potential risks.”
Interpreting and Using Results

“Collective risk assessment results can be used to corroborate conclusions, assemble a comprehensive risk-based plan and illustrate a bird’s eye view of AML risk within the enterprise.”

Data Quality Checks

Results can be reviewed for whether:
- Risk and control ratings make sense at a high level
- Final risk ratings align with individual risk and control ratings
- Ratings are consistent with auditor knowledge
- Any noticeable outliers or anomalies are present
- Particular assessments appear less supported than others

Comprehensive Risk-based Coverage for Audit Planning

Results can be used to inform planning decisions based on:
- Risk ratings & scores (e.g., highest risks areas)
- Identified risk trends (e.g. areas of increasing risk)
- Line of business or other organizational structures
- Geography
- Central functions/utilities
- Common risks and control weaknesses
- Prior coverage (e.g., audit testing, regulatory exams)

Enterprise Views of AML Risk

Results can be aggregated and viewed at various levels to:
- See whether results align with current expectations
- Identify explanations for any deviations from expectations
- Determine whether unexplained results warrant further escalation and/or exploration
Collective risk assessment data can be organized, stratified and dissected in a number of ways to create a variety of views for reporting and analysis.

<table>
<thead>
<tr>
<th>Line of Business</th>
<th>Country</th>
<th>AML Risk Trend</th>
<th>Prior Coverage</th>
<th>Customers</th>
<th>Products and Services</th>
<th>Transaction Activity</th>
<th>Geographic Presence</th>
<th>Know Your Customer</th>
<th>Suspicious and/or Unusual Activity</th>
<th>OFAC and Sanctions</th>
<th>Staffing and Training</th>
<th>Oversight and Governance</th>
<th>Operations and Technology</th>
<th>Policies, Procedures, Processes</th>
<th>AML SCORE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Unit A</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
</tr>
<tr>
<td>Business Unit B</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
</tr>
<tr>
<td>Business Unit C</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
</tr>
<tr>
<td>Business Unit D</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
<td>&quot;_&quot;</td>
</tr>
</tbody>
</table>
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.

Design the tool to:
- Direct auditors towards relevant considerations
- Facilitate thoughtful analysis
- Encourage supported conclusions

Establish a Support Framework with:
- Subject matter expertise
- Continual training and guidance
- Planning for supporting data
- Direction for crafting strong narratives

Takeaway
The risk assessment design can better equip Audit.
Bio
Jonathan Estreich is currently a vice president within the internal audit department at JPMorgan Chase. With over nine 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:
- Advanced Anti-Money Laundering Audit designation (CAMS-Audit)
- Certified Anti-Money Laundering Specialist (CAMS)
- Certified Fraud Examiner (CFE)
- Certified Associate in Project Management (CAPM)

Related Works by Author
- 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).
- Understanding recent developments in prepaid access: Considerations for deterring money laundering, ACAMS Today, (March 2012).
- “Knowing” your Latin American customer: Enhanced due diligence practices to mitigate the risks of money laundering and terrorist financing, InsideCounsel, (March 2012).
- Enhanced due diligence program for correspondent banking: Minimizing the risk of money laundering and drug trafficking, Thomson Reuters Complinet, (August 2011).