ACAMS RISK ASSESSMENT™

ACAMS®

Anti-Money Laundering Risk Assessment Methodology

06/16/2021

Version 6.1

Table of Contents

1. Introduction

ACAMS Risk Assessment™ (RA) is designed with the premise that under current regulatory environments and recent enforcement actions, financial institutions are in need of an industry standard to assess the broad range of money laundering (ML) risks. The ACAMS RA Tool was created to respond efficiently and appropriately to the guidance provided by global authoritative sources on the prevention and detection of financial crimes. This document starts with the specification of the methodology for assessing the inherent money laundering risk of products, services, delivery channels, high risk and prohibited customer and entity types, as well as high risk and prohibited geographies associated with financial institutions.

ACAMS Risk Assessment's methodology provides the basis to better understand the potential inherent ML risks that may arise within an institution's wide range of products and services, customer types, and geographic exposures, allowing the opportunity for the development and implementation of appropriate preventative and detective controls throughout a product's life cycle.

Such controls, may include, but are not limited to:

- Appropriate coverage of KYC requirements, including robust ID verification policies and procedures;
- Terms and conditions to enforce prohibitions and introduce limits;
- Policies and procedures that identify, confirm (or not), and process sanctions matches and that prevent any form of relationship or transactions with sanctioned entities;
- Monitoring rules aimed at detecting unusual transaction patterns and customer activity that deserve an explanation and may be suspicious and reportable.

The ACAMS AML Risk Assessment Methodology relies on a series of AML Risk tool components. These tools and their components are based on information that is objective, verifiable, and derived from globally recognized, authoritative sources. (See Appendices for detailed descriptions.)

The end result of employing the ACAMS methodology is an estimation of a financial institution's residual ML risk related to each of its products/services, customer types, and geographies, plus its average residual ML risk.

2. Implementing the AML Risk Assessment Methodology

Step 1

The first step ACAMS uses in determining the potential money laundering risks at an institution is to identify the level of risk based on the following three different questionnaire and flowchart-based tools:

- PRODUCTS, SERVICES, AND DELIVERY CHANNELS
- HIGH RISK AND PROHIBITED INDIVIDUAL AND ENTITY CUSTOMER TYPES
- HIGH RISK AND PROHIBITED GEOGRAPHIES

The table below provides some examples of the sorts of items/matters considered under each tool component.

ACAMS ML Risk Assessment – Examples of Tool Components

All Products & Services	Prohibited and/or High-Risk Customer Types/Entity Types	Prohibited and/or High-Risk Geographies
Savings Accounts	**Politically-exposed persons** (and relatives and close associates - per FFIEC)	**Prohibited Jurisdictions** (as stipulated by authoritative sources or determined by a financial institution's own policy)
Term Deposits / CDs and Money Market Funds	**Non-resident aliens** (per FFIEC).	**FATF-designated jurisdictions that FATF calls on its members to apply counter-measures**
ACH Transactions - Domestic (Involvement as ODFI and/or RDFI)	**Shell banks**	**FATF-designated jurisdictions with strategic deficiencies that have not made sufficient progress or have not committed to an action plan**
Domestic Correspondent Accounts - Funds Transfers (both international and domestic)	**Multi-level pyramid selling enterprises**	**Jurisdictions experiencing serious political/economic turmoil**
Non-Deposit Investment Products (securities, bonds, fixed income and variable annuities offered to customers who do not need to be customers of the FI) - **Direct Sales** -- either co-branded or through dual-employee arrangements	**Internet adult content sites and providers**	**INSCR Countries of Primary Concern that do not have sufficient AML/AFT regulations**
Demand Deposit Accounts = An account from which deposited funds can be withdrawn at any time without any notice to the depository institution [Note: DDAs are often associated with debit cards, check-writing (checkbooks), check cashing (including personal checks, business checks, TCs, MOs). Accounts may also be accessed and used via provision of e-banking (see separate discussion.)]	**Money service businesses (including: (a) currency dealers/exchangers/casas de cambio; (b) check cashers; (c) issuers of traveler's checks, money orders, stored value; (d) sellers/redeemers of traveler's checks, money orders, stored value; and (e) money transmitters.)**	
Consumer Credit Cards	**Casinos and other gaming activities**	
Payday Loans (= loans secured on the	**Cash-intensive businesses**	

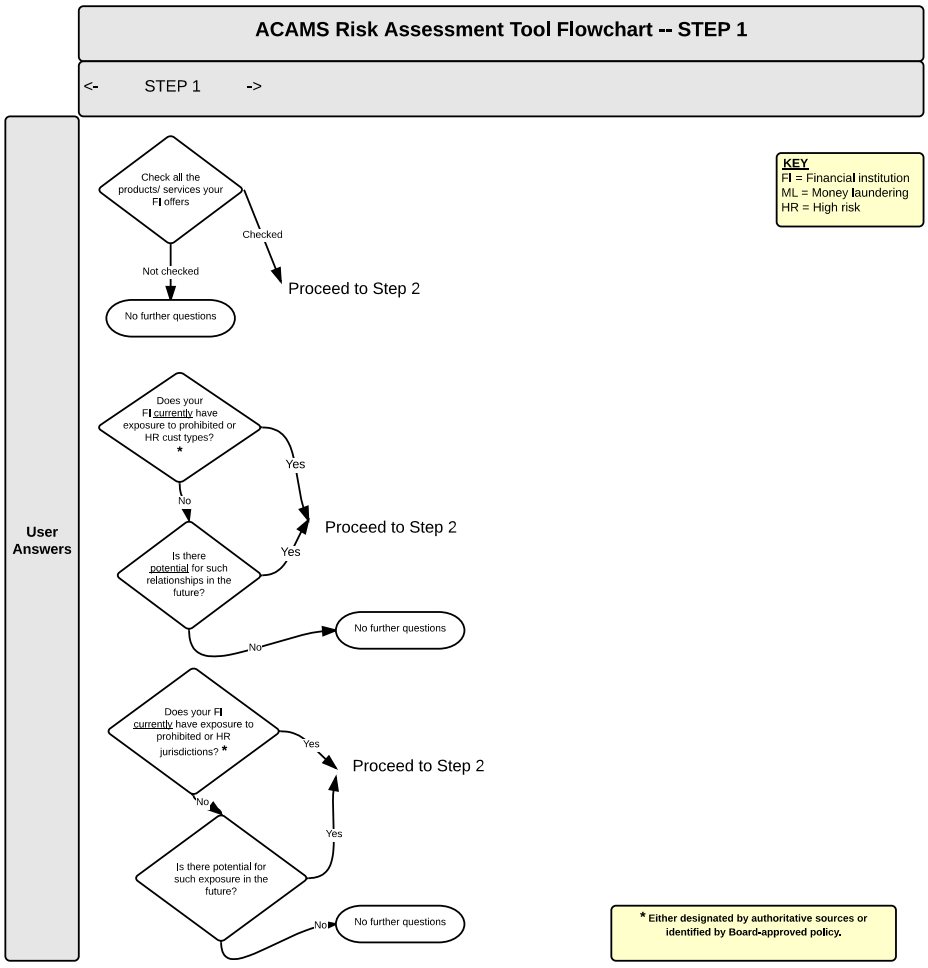
basis of expected payroll checks)		
Corporate Travel and Expense Card Products [These products involve arrangements with corporate customers, whereby the corporation's employees are provided credit/charge cards, often co-branded. Payment responsibility may either be the corporation's or the employee's.]	**Dealers in high-value precious goods, antiques, auction houses, estate agents**	
Virtual Currency	**Real estate businesses (per FATF paper)**	

The application of the ACAMS AML Risk Assessment Methodology starts with the Products/Services Tool. Within this tool, the user selects all applicable products and services. Each product/service the user designates has been pre-assigned an inherent money laundering risk score. This score is based on an assessment of the product's/service's core features and their attractiveness to money launderers evaluated against the following six key risk dimensions – involvement of cash or cash-equivalent monetary instruments; anonymity; rapid value funds movement; large value funds movement; cross-border funds movement; and involvement of unrelated 3rd parties. **[Note: Appendix 1 describes in detail the derivation of and background for the inherent risk scores for all products/services.]**

Next, the ACAMS AML Risk Assessment Methodology runs the user through processes related to Customer/Entity Types and Geographies. The main "Step 1" question for both of these is whether or not the user's financial institution has actual or potential exposure to either Prohibited or High-Risk customer types (individuals or entities) OR Prohibited or High-Risk geographies. Thus, for example, the user may indicate that they currently have no relationships with casinos or with Nigeria but that there are no circumstances or policies preventing such relationships in the future.

The diagram below summarizes the process flow through Step 1 of each of the tools. The completion of Step 1 leads to the comprehensive evaluation of the user's money laundering risk contained in Step 2.

Flowchart for Step 1 of ACAMS RA Methodology



Step 2

Having completed Step 1, the ACAMS AML Risk Assessment Methodology introduces the user to the detailed questions related to internal preventative and detective controls for each of the categories that have been checked. The outcome of Step 2 is the calculation of residual risk scores for products/services, customer types, and geographies.

Step 2 Questionnaire Sections:

A. Products/Services Risk Assessment

For all products/services selected by the user in Step 1 and for all the relevant features of those products/services within the six key risk dimensions, the user is guided through a series of questions related to internal preventative and detective controls that may be applied to mitigate risk. Thus, starting with a product's/service's inherent money laundering risk score, and considering the internal risk mitigation controls specified by the user, a residual money laundering risk score for that product/service can be calculated.
After the user has completed questions on all specified products/services, the ACAMS tool will identify an OVERALL PRODUCT/SERVICE MONEY LAUNDERING RISK SCORE. ACAMS utilizes the principle of the "weakest link" to identify this score – that is, an institution's overall product/service money laundering risk score reflects the highest (or worst) residual risk among its set of products/services.

Table below that graphically depicts the process described above.

Product	Risk Dimension (with base inherent risk score related to specific core and incidental features of the product)	Internal Preventative Controls (specific to product features)	Internal Detective Controls (specific to product features)	Residual Risk (for each Risk Dimension)
Product "X"	Involves cash or cash equivalent monetary instruments (base score = max 20)	Subtracts from score.	Subtracts from score.	Residual score (max = 20, min = 0)
	Supports anonymity (base score = max 20)	Subtracts from score.	Subtracts from score.	Residual score (max = 20, min = 0)
	Supports rapid value transfer (base score = max 20)	Subtracts from score.	Subtracts from score.	Residual score (max = 20, min = 0)
	Supports large value transfer (base score = max 20)	Subtracts from score.	Subtracts from score.	Residual score (max = 20, min = 0)
	Supports cross-border value transfer by (base score = max 20)	Subtracts from score.	Subtracts from score.	Residual score (max = 20, min = 0)
	Involves unrelated 3rd parties by (base score	Subtracts from score.	Subtracts from score.	Residual score (max = 20, min = 0)

	= max 20)			
	Starting inherent risk score (= sum of scores from each relevant risk dimension = max 120)			Final calculated residual risk score (max = 120, min = 0) with result designated as High, Medium, or Low

In addition to the calculation of the residual money laundering risk for each product/service that the user has specified, the ACAMS tool provides the user with the ability to then input their evaluation of the effectiveness of each of the controls as it relates to nine standardized control factors. The current strength of control factors that the Tool considers may be used to determine the effectiveness of an institution's AML program controls and are as follows:

a. **Management Oversight & Accountability:** Level of engagement, acute awareness of AML responsibilities, and management of ML risks from both Board of Directors and Senior Management
b. **Policies & Procedures:** such as adherence and documentation of all BSA/AML programs, policies and procedures
c. **Compliance Training:** Including a written, Board approved program that meets relevant standards for content, employee coverage, attendance, and adequate frequency.
d. **Systems & Operations:** Availability, stability, and complexity of operations, systems, and products such as those used for transaction monitoring
e. **Business Unit Monitoring & QA:** Business unit monitoring and quality assurance including proper systems for checks and balances
f. **Regulatory Environment:** MRAs, prior issues, past examinations, regulatory reporting
g. **Personnel Risk:** Provide for sufficient controls to ensure employee accountability. Perform adequate supervision of employees that handle currency transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity covered by the BSA and other AML requirements. Proper monitoring of management or employees that disregard established AML policies, procedures, as well as reasonable frequency in monitoring of the individual's intent and ability to adhere to AML program requirements, reporting, and registration and recordkeeping requirements.
h. **Independent Testing:** of all management systems and controls including but not limited to adequacy of transaction monitoring, adequacy of suspicious activity reporting and monitoring, and adequacy of employee knowledge and training programs
i. **Audits/Reviews:** both internal and external

It is important to note that the evaluation of control factor effectiveness does not automatically affect the final residual numerical score as it is left to the FI to determine and weigh the results of the evaluation against the FI's overall risk. If the FI determines that a control factor for a particular feature control is "ineffective" or "needs improvement", then that product, customer entity or jurisdiction category will be flagged accordingly, and both numerical score and classification will remain unchanged. If FI should desire to change the numerical score/classification based on control effectiveness, FI has the ability to change the final residual score based on the assessment of the controls as described above. See ***Appendix 4 - Guidance on Determining Strength of Controls based on Standardized AML Control Factor Evaluation*** for scoring method and scoring guidance as it relates to control effectiveness.

The next step is to then (a) to enter quantitative details on the product/service; and (b) indicate whether risk is expected to increase, decrease, or remain flat, and to indicate an action plan to lower the residual money laundering risk for that product/service further through improved preventative and detective controls. [Note: These additional entries do not affect directly the original residual risk scores calculated by the ACAMS tool. However, these entries will play an important role (a) to provide summary reporting for internal and external audiences and (b) to lend perspective to the potential impact of various products/services in order to apply appropriate controls based on the risk profile of the institution.]

B. Customer/Entity Types Risk Assessment

The Individual Customer/Entity Type Customer Tool asks the user about internal preventative and detective controls related to PROHIBITED individual customers (e.g., sanctions matches) and structure/industry/business entity customer types (e.g., sanctions matches, shell banks, etc.) designated by authoritative sources. In addition, the tool asks the user about individual or entity types that Board-approved policy may have designated as PROHIBITED (e.g., entities on which SARs have been filed, "Do Not Do Business With" Lists, etc.). Depending on the user's answers regarding internal controls related to prohibited relationships, a residual risk score will be calculated.

For HIGH-RISK individual customers (e.g., PEPs, Non-Resident Aliens) and structure/industry/business entity customer types (e.g., trust-like structures, cash intensive businesses, MSBs, casinos, unregulated charities, etc.) with which the user has identified current or potential relationships, the ACAMS tool asks questions about relevant internal preventative and detective controls. Depending on the user's answers regarding internal controls related to their high-risk relationships, a residual risk score will be calculated.

After the user has completed questions on all specified customer and entity types, the ACAMS tool will identify an OVERALL CUSTOMER/ENTITY TYPE MONEY LAUNDERING RISK SCORE. ACAMS utilizes the principle of the "weakest link" to identify this score – that is, an institution's overall customer/entity type money laundering risk score reflects the highest (or worst) residual risk among its set of customer relationships.

As with the Products/Services Tool, in addition to the calculation of the residual money laundering risk for each customer type with which the user has relationships, the ACAMS tool provides the user with the ability: (a) to evaluate the effectiveness of internal control factors b) to enter quantitative details on the customer types; and c) to indicate direction of risk as well as an action plan to lower the residual money laundering risk for those relationships further through improved preventative and detective controls. [Note: These additional entries do not affect directly the original residual risk scores calculated by the ACAMS tool. However, these entries will play an important role (a) to provide summary reporting for internal and external audiences and (b) to lend perspective to the potential impact of various customer relationships in order to apply appropriate controls based on the risk profile of the institution.]

See table below that graphically depicts the process described above.

Customer Type	Internal Preventative Controls	Internal Detective Controls	Residual Risk
Prohibited Customer Type "Y" (with default maximum score of 120)	Specific internal controls (subtract a maximum of 60 points)	Specific internal controls (subtract a maximum of 60 points)	120 starting points – points for specific preventative and detective controls indicated by user = residual risk score (which results in designation as High, Medium, or Low)
High-Risk Customer Type "Z" (with a default maximum score of 120)	Specific internal controls (subtract a maximum of 60 points)	Specific internal controls (subtract a maximum of 60 points)	120 starting points – points for specific preventative and detective controls indicated by user = residual risk score (which results in designation as High, Medium, or Low)

C. Geographic Risk Assessment

The Geography Risk Tool asks the user about internal preventative and detective controls related to PROHIBITED foreign and domestic geographies either designated by authoritative sources (OFAC, UK government, UN) or by Board-approved policy. Depending on the user's answers regarding internal controls related to prohibited geographies, a residual risk score will be calculated.

For HIGH-RISK foreign and domestic geographies, the ACAMS tool asks questions about relevant internal preventative and detective controls. Depending on the user's answers regarding internal controls related to their associations with high-risk geographies, a residual risk score will be calculated.

After the user has completed questions on all associated geographies, the ACAMS tool will identify an OVERALL GEOGRAPHIC MONEY LAUNDERING RISK SCORE. ACAMS utilizes the principle of the "weakest link" to identify this score – that is, an institution's overall geographic money laundering risk score reflects the highest (or worst) residual risk among its set of geographic associations.

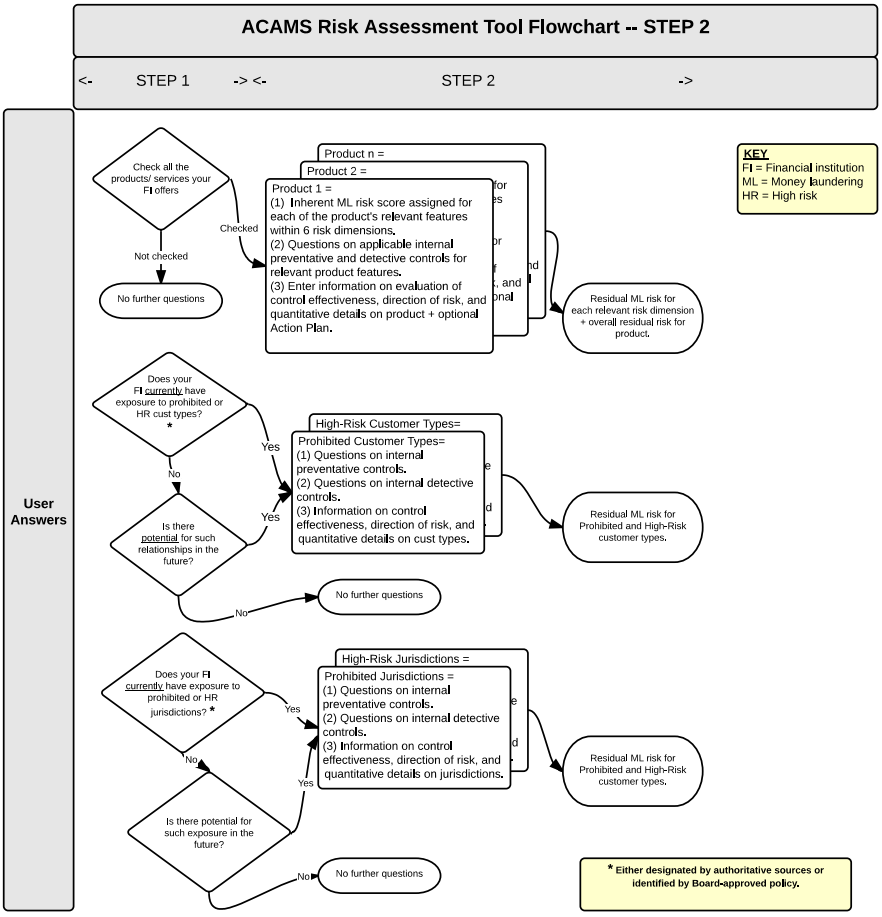
As with the Products/Services tool, in addition to the calculation of the residual money laundering risk for each High-Risk foreign or domestic geography with which the user has relationships, the ACAMS tool provides the user with the ability: (a) to evaluate the effectiveness of internal control factors b) to enter quantitative details on the customer types; and c) to indicate direction of risk as well as an action plan to lower the residual money laundering risk for those relationships further through improved preventative and detective controls. [Note: These additional entries do not affect directly the original residual risk scores calculated by the ACAMS tool. However, these entries will play an important role (a) to provide summary reporting for internal and external audiences and (b) to lend perspective to the potential impact of various geographic exposures in order to apply appropriate controls based on the risk profile of the institution.]

Table below that graphically depicts the process described above.

Jurisdiction	Internal Preventative Controls	Internal Detective Controls	Residual Risk
Prohibited Geography "Y" (with default maximum score of 120)	Specific internal controls (subtract a maximum of 60 points)	Specific internal controls (subtract a maximum of 60 points)	120 starting points – points for specific preventative and detective controls indicated by user = residual risk score (which results in designation as High, Medium, or Low)
High-Risk Geography "Z" (with a default maximum score of 120)	Specific internal controls (subtract a maximum of 60 points)	Specific internal controls (subtract a maximum of 60 points)	120 starting points – points for specific preventative and detective controls indicated by user = residual risk score (which results in designation as High, Medium, or Low)

The diagram below summarizes the process flow through Step 2 of each of the component tools. The completion of Step 2 leads to the evaluation of the user's overall money laundering risk contained in Step 3.

Flowchart for Step 2 of ACAMS RA Methodology



Step 3

A fundamental concept of our ACAMS tool is that, after completion of the questionnaire, a user will receive an "overall" ML risk score for each category/individual risk tool. Users have the right to expect that our tool will provide a valid and valuable perspective on how their AML risk management program stands in addressing the risks it faces in its products/services, customers, and geographic exposures. This information is critical in informing an institution's Executives, Board of Directors, and regulators and in directing an institution's efforts to manage its AML risks through internal preventative and detective controls.

Thus, after completion of Steps 1 and 2 above, the ACAMS AML Risk Assessment Methodology carries the process to its logical conclusion by providing the user with a final Average RESIDUAL MONEY LAUNDERING RISK SCORE by category/individual risk tool. As described earlier, ACAMS utilizes the principle of the "weakest link" to identify the inherent risk score – and institutions can derive the same for an overall average. That is, an institution's final average money laundering risk score that is derived from an inherent risk score representing the weakest link and then the application of internal controls resulting in a final residual risk score.

It is important to note that the average overall risk score that is derived from each individual risk tools that utilize the principle of the "weakest link" to identify this score – that is, an institution's final average money laundering risk score reflects internal components that have at the core, the highest (or worst) inherent risk from its individual risk tools.

The ACAMS recommendation, is that a financial institution's Overall AML Residual Risk should default to the Residual Risk of their highest product, geographic, or customer risk. Thus, if at the completion of our ACAMS tool, an institution has a product, geographic exposure, or customer type with a Residual Risk of HIGH, the institution's Overall AML Residual Risk should be viewed as HIGH, regardless of the associated metrics.

Our rationale is that this approach does not disguise or dilute what may be considered an unpleasant reality – that is, that the institution's AML risk management is flawed or incomplete enough to result in an area that possesses HIGH residual risk.

An institution has the option of disagreeing with the our tool's Residual Risk result(s) for entirely legitimate reasons – for example, (1) the high-risk product in question is being sunsetted and no new accounts are being accepted or (2) policies and procedures are being introduced (but are not in effect yet) that obviate risks because of new prohibitions and controls.

If institutions opt to do this, then their rationale for disagreeing with our tool's HIGH residual risk score will be clearly articulated and transparent to all, including their BOARD and regulators.

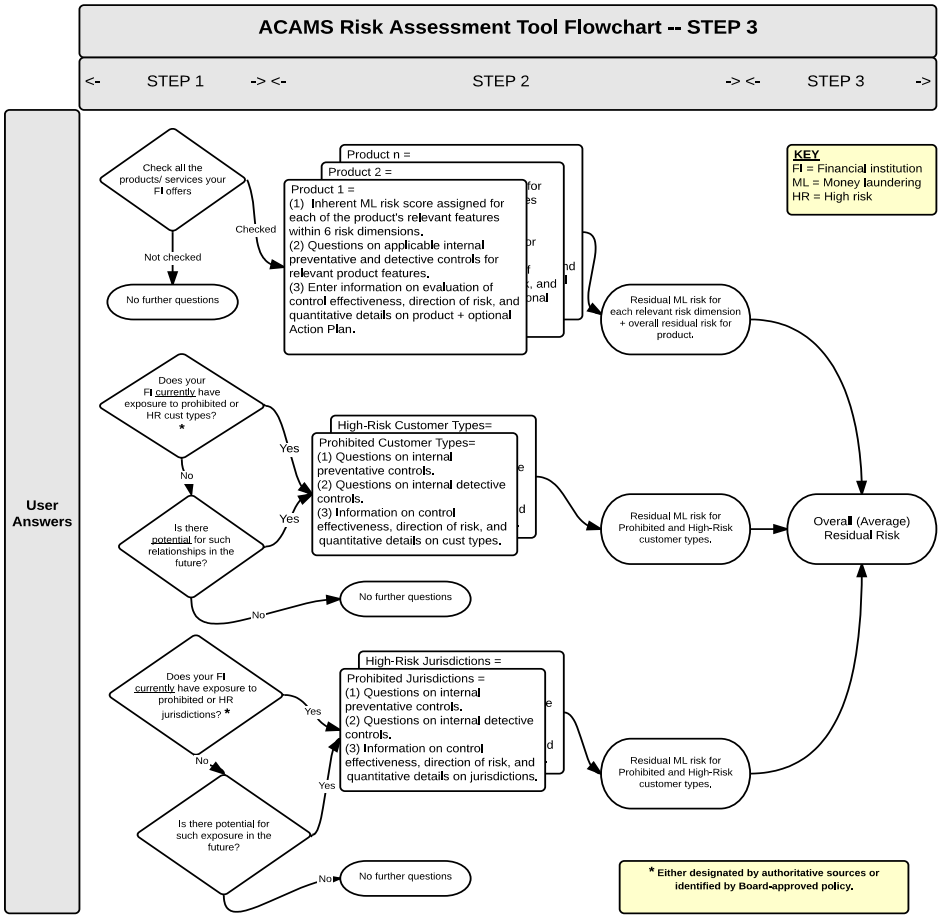
To illustrate the efficacy of and need for a Residual Risk approach that does not rely entirely on metrics and one that does not disguise or dilute an institution's overall residual AML risk, we submit the following examples:

- Banks offering private banking, although the numbers of private bank customers were miniscule compared to their total customer base, have experienced failures in their private banking AML programs that have led to disruptive and costly enforcement actions.
- Other banks have had serious problems uncovered by examiners in their risk management programs related to PEPs and embassy accounts that have led to disruptive and costly enforcement actions, even though these customers represented a minimal proportion of their customer base.
- Still other banks were shown to have participated in international bulk currency shipments involving a high-risk jurisdiction. Again there were disruptive and costly enforcement actions taken by regulators, even though bulk shipment of currency was a relatively small sidelight business.

ACAMS contends that in all the examples above, the products and customer types in question would have represented a very small, even deceptively insignificant, portion of their respective institution's overall residual AML risk.

Please refer to the diagram below, which now summarizes all three steps in the ACAMS RA Methodology.

Summary Flowchart for ACAMS RA Methodology



Optional Suspicious Activity Risk Assessment Module

Introduction and Objective

Per international standards, a fundamental component of a country's Anti-Money Laundering/Anti- Terrorist Financing program is a robust suspicious activity reporting regime. As a result, financial institutions and other covered entities are expected to have their own programs to meet their country's legal and regulatory requirements to identify and report suspicious activity. The fundamental authoritative source vis-à-vis suspicious activity reporting comes from the Financial Action Task Force (FATF) and its "40 Recommendations" – "Recommendation 20 – Reporting of suspicious transactions." This recommendation states:

> "If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU)."

In response to the FATF Recommendation #20, most of the world's jurisdictions, including all of the major banking nations, have adopted rigorous suspicious activity reporting regimes. Examples include:

- In the US, the Financial Crimes Enforcement Network (FinCEN) regulates Suspicious Activity Reports (SARs), and, based on FinCEN regulations, the Federal Financial Institutions Examination Council's (FFIEC's) "Bank Secrecy Act/ Anti-Money Laundering Examination Manual" identifies in detail the government's expectations of SAR programs and how they will be examined.
- In Canada, the Financial Transaction and Reports Analysis Centre (FINTRAC) regulates Suspicious Transaction Reports (STRs) as well as provides guidance to covered financial institutions and entities on the government's expectations of STR programs.
- In Australia, the Australian Transaction Reports and Analysis Centre (AusTRAC) regulates Suspicious Matter Reports (SMRs) as well as provides guidance to covered financial institutions and entities on the government's expectations of SMR programs.
- In Singapore, the Monetary Authority of Singapore regulates Suspicious Transaction Reports (STRs) as well as provides guidance to covered financial institutions and entities on the government's expectations of STR programs.

Regulatory oversight in the above jurisdictions includes examinations to assure compliance with the laws and regulations governing suspicious activity reporting. **The objective of the ACAMS Risk Assessment Tool's "Suspicious Activity Reporting Program Risk Module" is to provide Users the ability to evaluate and report on their residual risk as it relates to their Suspicious Activity Reporting (SAR) programs.** [As noted above, these programs are known by various other names (e.g., SMR, STR), but all are focused on the reporting of unusual/suspicious financial activity to competent authorities in a country.]

Suspicious Activity Risk Module Process

The Suspicious Activity Reporting Program Risk Module Process involves the following steps:

(1) Users identify all applicable suspicious activities/transactions/crimes on which their financial institutions are obligated to report;
(2) For all of those activities/transactions/crimes that are checked, Users are asked questions about their use of Preventative Controls (PCs) and Detective Controls (DCs) to mitigate the risk associated with the reporting of suspicious activities;
(3) For all the PCs and DCs that the User identifies that they are using, the User is asked questions about the strength of these controls;
(4) At the end of the process, the User is provided both (a) a specific view of the Residual Risk related to each activity/transaction/crime for which they have exposure and (b) a recommended view of the overall Residual Risk for their suspicious activity reporting program;

The ACAMS RA Tool's approach to this module is to make it as adaptive as possible to the wide range of needs reflected in multiple jurisdictions. That is, the RA Tool's module includes specific suspicious activity/transaction/crime reporting requirements reflected in multiple jurisdictions. The PCs and DCs that accompany each reportable suspicious activity/transaction/crime category are based on international authoritative sources that identify expected best practices in the prevention and detection of suspicious activity.

<u>STEP 1 - An exhaustive list of possibly applicable suspicious activities/transactions/crimes</u>

In order for the ACAMS RA Tool's "Suspicious Activity Reporting Program Risk Module" to be as broadly applicable as possible across jurisdictions, the module includes all the covered crimes alluded to in the suspicious activity/transaction regulations of multiple jurisdictions. Examples include:

- The SAR form administered by FinCEN in the US identifies over 100 specific underlying crimes (and associated financial products) related to money laundering and terrorist financing that it requires covered financial institutions and entities to report on, including:
    - Seven subtypes of financial transaction structuring;
    - Sixteen subtypes of fraud (including 5 types of mortgage fraud);
    - Fives types of suspicious transactions at casinos;
    - Thirteen types of financial transactions that are "red flags" indicating possible money laundering;
    - Six different activities involving identification/documentation practices that might be suspicious;
    - Seven different insurance transactions that may be suspicious;
    - Six securities/futures/options transactions that may be suspicious.
- Among others, the jurisdictions of Hong Kong, Singapore, Canada, and Australia require reporting activities/transactions that might indicate tax evasion.
- Singapore specifically identifies "419/Advance fee/Nigerian scams" as a form of fraud to be reported.
- Singapore and Australia require reporting activities/transactions that may be related to immigration-related offenses, as well as human smuggling.
- Singapore requires reporting on reporting activities/transactions that might be related to kidnapping.
- Singapore requires reporting on reporting activities/transactions that might be related to "dealing in obscene or other objectionable material."

The RA Tool's "Suspicious Activity Reporting Program Risk Module" will include all of the above, and the User is **only** required to answer questions related to those activities/transactions/crimes relevant to their jurisdiction.

STEP 2 - Applicable Preventative and Detective Controls

As previously indicated, the PCs and DCs that accompany each reportable suspicious activity/transaction/crime category are based on international authoritative sources that identify expected best practices in the prevention and detection of suspicious activity. Among others, these sources include:

- FATF's "Interpretive Notes to Recommendation 20 (Reporting of Suspicious Transactions)";
- The FFIEC's "Bank Secrecy Act/ Anti-Money Laundering Examination Manual";

- AusTRAC's "AML/CTF Rules (chapter 18)";
- The Singapore Monetary Authority's "Notice on Reporting of Suspicious Activities and Incidents of Fraud."

The ACAMS RA Tool's "Suspicious Activity Reporting Program Risk Module" distills these best practices to the following basic PCs and DCs:

Preventative Controls expected:

- (1) Documented policies, procedures, and processes (promulgated by properly designated authority) should be in place to identify and monitor for this particular activity, which may be suspicious and reportable to government authorities; AND (2) an appropriate number of well-trained staff to identify, research and report this particular suspicious activity.

Detective Controls expected:

- (1) Processes for the FI staff to identify and report **internally** instances of this particular activity; AND (2) appropriate manual or automated monitoring systems designed to highlight unusual activity that deserves an explanation and that may involve this particular activity.

STEP 3 – Evaluation of the strength of Preventative and Detective Controls

The User is next asked to evaluate the strength of the PCs and DCs that were identified as part of their Suspicious Activity Reporting program, based on nine categories of effectiveness. Among other authoritative sources for these nine categories, ACAMS cites the Wolfsberg Group's 2015 document, "The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions, and Bribery & Corruption."

These nine categories of effectiveness are:

- **Management Oversight & Accountability:** Level of engagement, acute awareness of AML responsibilities, and management of ML risks from both Board of Directors and Senior Management.
- **Policies & Procedures:** Such as adherence and documentation of all BSA/AML programs, policies and procedures.
- **Compliance Training:** Including a written, Board approved program that meets relevant standards for content, employee coverage, attendance, and adequate frequency.

- **Systems & Operations:** Availability, stability, and complexity of operations, systems, and products such as those used for transaction monitoring.
- **Business Unit Monitoring & QA:** Business unit monitoring and quality assurance including proper systems for checks and balances.
- **Regulatory Environment:** MRAs, prior issues, past examinations, regulatory reporting.
- **Personnel Risk:** Provide for sufficient controls to ensure employee accountability. Perform adequate supervision of employees that handle currency transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity covered by the BSA and other AML requirements. Proper monitoring of management or employees that disregard established AML policies, procedures, as well as reasonable frequency in monitoring of the individual's intent and ability to adhere to AML program requirements, reporting, and registration and recordkeeping requirements.
- **Independent Testing:** of all management systems and controls including but not limited to adequacy of transaction monitoring, adequacy of suspicious activity reporting and monitoring, and adequacy of employee knowledge and training programs.
- **Audits/Reviews:** Both internal and external.

[Note: Please refer to Appendix 4 – "Guidance on Determining Strength of Controls based on Standardized AML Control Factor Evaluation."]

STEP 4a - Derivation of Residual Risk for each applicable suspicious activity/transaction/crime

The following formula represents the derivation of a Residual Risk score for each of the activities/transactions/crimes on which a financial institution is required to report:

SusAct RR = [120 – (PC + DC)]

Key

SusAct RR = Final Residual Risk for a Specific Suspicious Activity
PC = Preventative Control for Specific Suspicious Activity (including assessment of strength of controls)
DC = Detective Control for Specific Suspicious Activity (including assessment of strength of controls)

STEP 4b - The Residual Risk for overall Suspicious Activity Reporting Program

A fundamental concept of our ACAMS tool is that, after completion of each tool/module, a User will receive an "overall" ML risk score for each category. Users have the right to expect that our tool will provide a valid and valuable perspective on how their AML risk management program stands in addressing the risks it faces vis-à-vis their Suspicious Activity Reporting Program. This information is critical in informing an institution's Executives, Board of Directors, and regulators and in directing an institution's efforts to manage its AML risks through internal preventative and detective controls.

ACAMS recommends the utilization of the principle of the "weakest link" to identify the Residual Risk for overall Suspicious Activity Reporting Program. This means that a financial institution's Residual Risk for its overall Suspicious Activity Reporting Program should default to the Residual Risk of their highest Residual Risk score for any of the activities/transactions/crimes on which the financial institution is required to report. Thus, if at the completion of the module, an institution has a reportable activity/transaction/crime with a Residual Risk of HIGH, the institution's Overall SAR Program Residual Risk should be viewed as HIGH.

Our rationale is that this approach does not disguise or dilute what may be considered an unpleasant reality – that is, that the institution's AML risk management is flawed or incomplete enough to result in an area that possesses HIGH residual risk.

An institution has the option of disagreeing with the our tool's Residual Risk result(s) for entirely legitimate reasons – for example, policies and procedures are being introduced (but are not in effect yet) that mitigate risks associated with a particular activity/transaction/crime.

If institutions opt to do this, then their rationale for disagreeing with our tool's HIGH residual risk score will be clearly articulated and transparent to all, including their BOARD and regulators.

Optional Sanctions Risk Assessment Module

Introduction

The ACAMS Sanctions Program Risk Methodology is designed to respond to current regulatory environments and recent requirements to provide financial institutions with an industry standard (a) to assess the broad range of sanctions risks and (b) to manage those risks through best practices in Preventative and Detective Controls (PCs and DCs). The ACAMS Sanctions Program Risk Methodology was created to respond efficiently and appropriately to the guidance provided by global authoritative sources on sanctions risk management.

The foundations upon which a country's sanctions program should be based are: FATF Recommendation #6 ("Targeted financial sanctions related to terrorism and terrorist financing"); and FATF Recommendation #7 ("Targeted financial sanctions related to proliferation"). These FATF Recommendations and their Interpretive Notes are themselves based on UN Security Council resolutions regarding narcotics trafficking and proliferation.

Based on the UN/FATF principles, each compliant jurisdiction has created its own competent authority to oversee and administer its sanctions program. Examples include: in the US - the Office of Foreign Assets Control (OFAC); in Australia - the Department of Foreign Affairs and International Trade; in the UK - the Office of Financial Sanctions Implementation; in Canada - the Department of Foreign Affairs and International Trade; and in Singapore - the Monetary Authority of Singapore.

Authoritative sources for the Preventative and Detective Controls in the ACAMS Sanctions Program Risk Methodology include the following: (1) the US FFIEC 2014 BSA/AML Examination Manual's sections on "Office of Foreign Assets Control - Overview" and "Examination Procedures - Office of Foreign Assets Control"; (2) the UK Office of Financial Sanctions Implementation's "Financial Sanctions: Guidance" (April 2017); (3) the Monetary Authority of Singapore's "MAS Regulations issued pursuant to Section 27A of the MAS Act"; (4) Canada's Office of the Superintendent of Financial Institution's (OSFI's) issuances on sanctions. [**Note:** All the above sources follow the guidelines provided in the FATF's Recommendations and agree on the sanctions program requirements levied on their constituents.] Further, in 2019, the Wolfsberg Group issued "Guidance on Sanctions Screening", which further cemented the basic risk management requirements vis-à-vis name and transaction screening.

The ensuing section of this document illustrates how to implement the ACAMS Sanctions

Program Risk Methodology. The end result of employing the ACAMS methodology is an estimation of a financial institution's residual sanctions risk.

This result will be enhanced by the use of the ACAMS adaptation of the US FFIEC's "Quantity of Sanctions Risk" matrix (Appendix M in the FFIEC "BSA/AML Examination Manual"). ACAMS provides as an appendix to this document a process whereby a User can estimate the inherent "quantity of sanctions risk" at the outset of the assessment of their residual sanctions risk.

Implementing the ACAMS Sanctions Risk Assessment Methodology

Based on the above authoritative sources, the ACAMS Sanctions Program Risk Methodology has identified 17 expected program elements and best practices in preventative and detective internal controls (PCs and DCs) associated with each element.

It is the User's task to: (a) identify whether or not their institution has implemented the preventative and detective controls for each program element; and (b) to identify the strength of those controls.

Using our standardized approach, each program element has an inherent risk score of 120 points. Based on the existence of the prescribed PCs and DCs and the self-evaluated strength of those controls, the User subtracts an appropriate number of points (a maximum of 60 points for PCs and 60 points for DCs) to derive a residual score.

Example 1

Program element #1 = Development of a risk-based approach to designing and implementing a Sanctions Compliance Program (Inherent risk = 120 points).

> **Preventative internal control** = Either (1) Internal completion of an assessment of the "Quantity of Sanctions Risk" matrix (e.g., the Quantity of Sanctions Risk Module and/or Appendix M of the US's FFIEC "BSA/AML Examination Manual"); and/or (2) use of appropriate external Sanctions Program specialists to assess such risks.
>
> > If the User identifies that their institution has completed either (1) and/or (2), the User must then perform an evaluation of the nine control factors associated with that control, and manually implement any resulting risk point reduction score changes as necessary.

Detective internal control = Internal audit review and assessment of adequacy of relevant sanctions program risk assessment.

If the User identifies that their institution has the control in place, the User must then perform an evaluation of the nine control factors associated with that control, and manually implement any resulting risk point reduction score changes as necessary.

Example 2

Program element #7 = At the outset of any relationship (client take-on), sanctions checks should be made on all account parties. (Inherent risk = 120 points).

Preventative internal control = Board/Senior Management-approved adoption of policies, procedures, and processes that assure at the outset of a relationship that all account parties are checked against sanctions lists, including: accountholders; beneficiaries; guarantors; principals; beneficial owners; nominee shareholders; directors; signatories; and powers of attorney.

If the User identifies that their institution has the prescribed control, the User must then perform an evaluation of the nine control factors associated with that control, and manually implement any resulting risk point reduction score changes as necessary.

Detective internal control = Internal audit or external review confirmation that all parties to new accounts are checked against sanctions lists before relationships are initiated OR within a reasonable period.

If the User identifies that their institution has the control in place, the User must then perform an evaluation of the nine control factors associated with that control, and manually implement any resulting risk point reduction score changes as necessary.

End Result

After having completed the assessment of each of the 17 expected program elements, the User will have a residual risk score for each of those program elements.

The **Sanctions Program Assessment Report** averages the 17 program element scores to derive an average Sanctions Program Residual Risk score. Thus:

> Program element #1 residual risk + Program element #2 residual risk + . . . Program element #17 residual risk = Total/17 = Average Sanctions Program Residual Risk.

Based on the ACAMS Risk Assessment principle of symmetry, the total possible maximum score of 120 points for each section is divided into thirds, with the following result:

> If the final score for a sanctions program element is between 0 and 39 points, then the Residual Sanctions Risk for that element may be assessed as LOW.
>
> If the final score for a sanctions program element is between 40 and 79 points, then the Residual Sanctions Risk for that element may be assessed as MEDIUM.
>
> If the final score for a sanctions program element is between 80 and 120 points, then the Residual Sanctions Risk for that element may be assessed as HIGH.

In the same way as the reporting functionality of the ACAMS Risk Assessment Tool, the reporting functionality of the ACAMS Sanctions Program Risk Methodology provides: (a) an overview that includes an executive snapshot, an overall risk assessment narrative, and a sanctions program summary; (b) if used, an initial/inherent "Quantity of Sanctions Risk" score against which the User can objectively and reliably assess its own Sanctions Program performance and residual sanctions risk; (c) sanctions program details for each program element; (d) a summary of control exceptions (i.e., opportunities for improvement in PCs and/or DCs); and (e) an action plan.

In conclusion, the ACAMS Sanctions Risk Assessment Methodology provides a framework for institutions to conduct comprehensive assessments. Users should be sure to thoroughly evaluate each of their institution's implemented controls using the nine provided control factors, and adjust their risk point reductions accordingly, as well as complete an assessment of all 17 sanctions program element sections, in order to objectively meet the global best practices of a sound sanctions risk management program.

Note on Tool Flexibility

The ACAMS RA Tool is flexible enough to allow a financial institution to designate certain categories/items as high-risk – that is, possibly overriding the default risk level offered by the Tool. In such cases, a residual AML risk score will also be determined after consideration of internal preventative and detective controls.

In addition, the Tool allows users to override the Tool's final determination of residual risk when the user has compelling reasons to do so. Currently, the Tool asks questions about the strength of Preventative and Detective Controls but does not yet automatically score the strength on controls in determining the final residual risk for products, customer types, or geographies. Appendix 4 provides guidance on how users should evaluate the strength of their controls based on standardized control factors.

One of the Tool's main values is to call attention to cases in which a specific item's residual risk is determined to be "High." Such situations indicate immediate opportunities for improvement that the subscribing financial institution can address.

The detailed individual risk components on which the Tool is based are contained in the Appendix. The component processes are notably transparent, and they are based on objective, verifiable, and globally recognized authoritative sources. It is ACAMS' intent to maintain and update these tool components and keep subscribers apprised of changes that reflect on their ability to administer a strong AML risk management program.

APPENDICES

Appendix 1 –

Product/Service/Delivery Channels AML Risk Tool Details

Appendix 2 –

Customer/Entity Type AML Risk Tool Details

Appendix 3 –

Geographic AML Risk Tool Details

Appendix 4 –

Guidance on Determining Strength of Controls based on Standardized Control Factor Evaluation

Appendix 5 –

AML Risk Tool Development, Oversight and Maintenance

Appendix 1 –

Product/Service/Delivery Channels AML Risk Tool Details

- Decision Tree
- Explanation of Risk Dimensions I – VI
- Inherent (Core Feature) Product Risk Scoring
    - Basic scoring concept
    - Full table of Inherent Risk for all Products
- Incidental Product Feature Scoring
- Effect of Internal Preventative and Detective Controls
- Final Product Residual Risk Calculation

Core versus Incidental Product Features

Since the ACAMS AML Risk Assessment Methodology starts with products and services, it is important to provide details on how the inherent AML risk for each product/service is derived. First, it is necessary to distinguish between core and incidental features of a product/service – that is:

- A core feature of a product is one that is intrinsic to the nature or function of that product – for example, a core feature of consumer credit card is that it involves rapid value transfer upon its regular, expected usage at a point-of-sale;

- An incidental feature of a product is an activity or transaction that can potentially be undertaken by the user if he/she selects to do so – for example, an incidental feature of a consumer credit card is that it can involve cross-border value transfer IF the user travels overseas AND decides with make an ATM cash withdrawal.
  [NOTE: In the examples above, the core feature involves a primary activity for which the cardholder obtained the credit card, while the incidental feature can be viewed as one the cardholder may use if he/she traveled overseas and happens to require some currency.]

Money Laundering (ML) Risk Dimensions and Attributes

Derivation of basic inherent ML risk involves an assessment of the product's/service's core features and their attractiveness to money launderers (and therefore concern to regulators, law enforcement, and financial institutions) evaluated against the following six key risk dimensions. These risk dimensions are:

(1) **Cash or cash-equivalent monetary instruments** -- The involvement of currency and/or bearer-negotiable monetary instruments as a core feature of a product or service is of heightened concern because they are widely accepted, easily transferred, and anonymous;

(2) **Anonymity** -- A product or service that is anonymous supports the goals of money laundering or financing of terrorism since anonymity helps disguise the source of funds;

(3) **Rapid value funds movement** -- A product or service that allows for the rapid transfer of value supports the goals of money laundering or financing of terrorism by quickly disassociating the sources of funds from their illicit connections thereby making the tracking of the funds more difficult;

(4) **Large value funds movement** -- The ability to use a product or service to transfer large value can support the goals of money laundering or financing of terrorism to efficiently consolidate funds through the layering processes;

(5) **Cross-border funds movement** -- The ability to use a product or service to transfer value across borders can support the goals of money laundering or financing of terrorism to hide the source of illicit funds, make funds available for illicit purposes, and make continued tracking of the illicit funds more difficult;

(6) **Involvement of unrelated 3rd parties** -- Most transactions occur among parties related to one another through personal or business connections; therefore, products or services that facilitate the possible transfer of funds to or from unrelated third parties or that make it extremely difficult to discern relationships among transaction counterparties pose heightened risk.

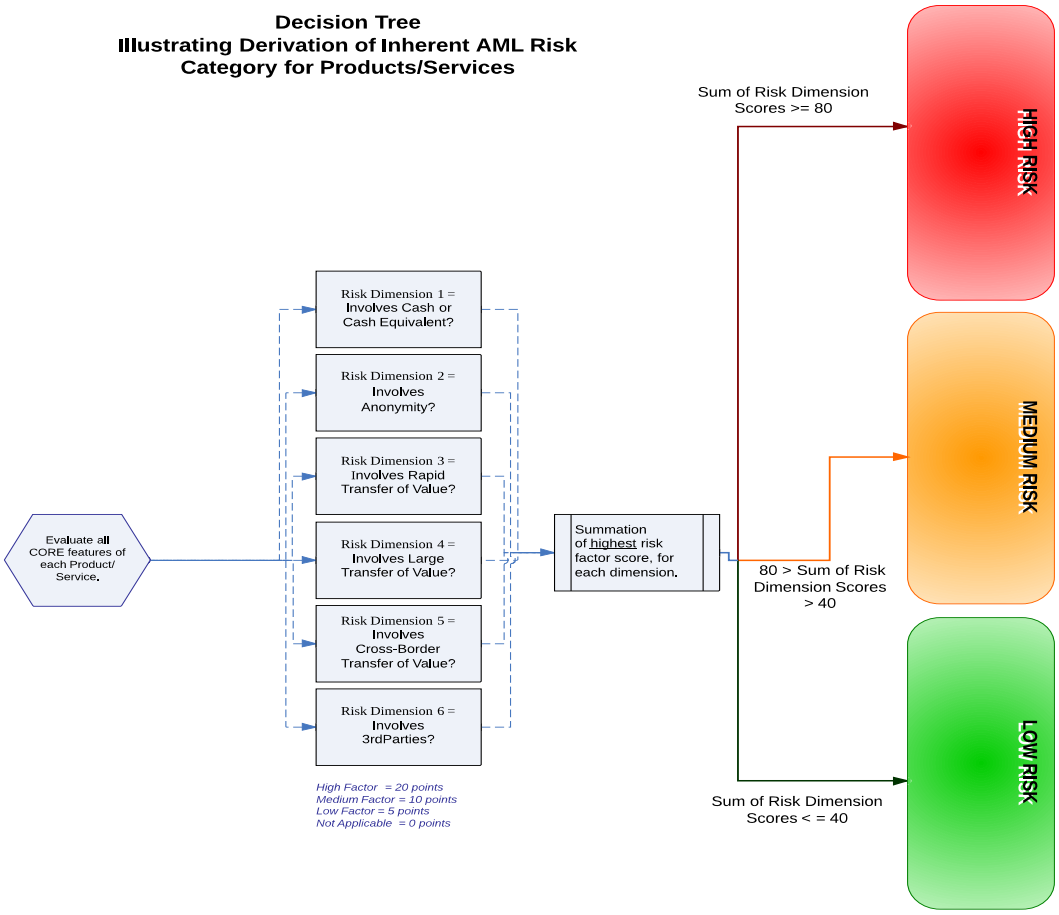
ACAMS has researched each of these risk dimensions, and, with the input from its Committee of Experts, has validated an array of attributes for each of these risk dimensions, rated from highest risk to lowest risk (and including the "Not Applicable" option). The six risk dimensions and their attributes are displayed in the table below:

Table - Risk Dimensions and Attributes and their Risk Ratings

Risk Flag Code	Risk Dimension and Attribute	Attribute Risk Rating
1 (a1)	**The following attributes (1(a1) - 1(d)) relate to the money laundering risk dimension of "involves cash."** Core feature of product/service is that it actually involves currency itself (e.g., forex cash-for-cash exchanges + ATM withdrawals).	High
1 (a2)	Core feature of product/service involves value in bearer-negotiable form (such as pre-paid card of any type).	High
1 (b1)	Product/service frequently involves value transfer in currency – i.e., cash IN + product/service OUT	Medium
1 (b2)	Product/service In + cash OUT. Examples include, traveler's check purchases or encashment, some forex transactions with other monetary instruments, some travel services.	Medium
1 (c)	Product/service may occasionally, but not characteristically, involve value transfer in currency.	Low
1 (d)	Not Applicable -- i.e., product does not involve currency in any direct manner.	N/A
2 (a1)	**The following attributes (2(a1) - 2(d)) relate to the money laundering risk dimension of "supports anonymity."** Core feature of product/service is that it is anonymous = i.e., little or no identification of the customer/holder is involved with product/service's use.	High
2 (a2)	Core feature of product/service is that there is little or no face-face interaction between customer/holder and the location where the product/service is being used (e.g., e-banking).	High
2 (a3)	Product/service can easily involve the concealment of beneficial ownership of funds/source of funds.	High
2 (b)	Product issued in specified party name, but may be transferred	Medium
2 (c)	<< there are no low AML risk flags >>	Low
2 (d)	Not Applicable -- i.e., anonymous acquisition and/or use of the product/service is not supported.	N/A
3 (a)	**The following attributes (3(a) - 3(d2)) relate to the money laundering risk dimension of "involves rapid value transfer."** Core feature of product/service is that it supports virtually real-time value transfer. Examples include most forms of electronic funds transfers.	High
3 (b1)	Product/service usually involves value transfer in near-term – i.e., within 1-3 days.	Medium
3 (b2)	Core feature of the product/service is immediacy of negotiability + wide acceptance.	Medium
3 (c)	Core feature of the product/service is immediacy of negotiability + narrow acceptance.	Low
3 (d1)	Not Applicable -- e.g., product/service does not involve real-time or near-term value transfer	N/A
3 (d2)	Not Applicable -- e.g., product/service has only limited/narrow acceptance.	N/A
4 (a)	**The following attributes (4(a) - 4(d2)) relate to the money laundering risk dimension of "involves large value transfer."** Product/service is NOT restrictive to easy transfer of large value	High
4 (b)	Product/service has restrictions/limits on value and frequency/timing that restrict transfers to less than $100,000 annually but > $25,000 annually.	Medium

4 (c)	Product/service has restrictions/limits on value and frequency/timing that restrict transfers to less than $25,000 annually.	Low
4 (d1)	Not Applicable -- i.e., product/service does not involve value transfer	N/A
4 (d2)	Not Applicable --	N/A
5 (a)	**The following attributes (5(a) - 5(d)) relate to the money laundering risk dimension of "involves cross-border value transfer."** Core feature of product/service is that it involves cross-border transfer of value – e.g., foreign wire transfers into/out of a country.	High
5 (b)	Although NOT a core feature of the product/service, it **FREQUENTLY** involves value transfer to/from a high-risk geography.	Medium
5 (c)	Although NOT a core feature of the product/service, it can allow possible cross-border transfer of value.	Low
5 (d)	Not Applicable -- i.e., product/service prohibits cross-border transactions.	N/A
6 (a)	**The following attributes (6(a) - 6(d)) relate to the risk dimension of "supports the possible involvement of 3rd parties."** Core feature of Product/service involves nested/obscured relationships (e.g., customers of our clients).	High
6 (b1)	Product/service funding may involve 3rd parties unrelated to the customer (e.g., via wire transfer, cash remittance, check)	Medium
6 (b2)	Product/service use may involve 3rd parties unrelated to the customer (e.g., encashment, use for POS transactions, use for ATM withdrawal, etc.)	Medium
6 (c)	Product/service available to non-account holders (i.e., entities that do not have a traditional customer relationship subject to CIP -- such as foreign exchange at an airport kiosk, travel services at an outlet/branch.)	Low
6 (d)	Not Applicable -- i.e., product/service restricted to customer of record.	N/A

Product/Service Inherent Risk Decision Tree



The flowchart/decision tree depicted above illustrates how each financial product/service is evaluated in order to derive its inherent AML risk score and rating. ACAMS has striven to reduce subjectivity to a minimum through the application of the following three principles:

(1) **The view that all six risk dimensions have the same value** (= attractiveness or appeal to a money launderer);
[**NOTE**: This perspective is supported by the notion that each single risk dimension, when viewed in isolation, has little value to a money launderer. It is truly the cumulative nature of a product's features that makes it worthwhile for the purposes of a criminal. For example, if the only features of a product are that it involves currency and is anonymous (but cannot support large value transfer, rapid value transfer, cross-border transfer, or unrelated 3rd parties), then the appeal of that product to a money launderer (and thus risk to a financial institution) is relatively LOW. On the other hand, if a product has attributes of a medium risk nature in all six dimensions, then the appeal to a money launderer (and risk to a financial institution) could be viewed as MEDIUM or HIGH, depending on the characteristics of the product. It seems unproductive to engage in a debate about possible relative differences in the values of each risk dimension.]

(2) **The application of the principle of symmetry in the assignment of scores to the HIGH, MEDIUM, and LOW risk attributes** – that is, the HIGH-RISK attributes have a score (in the ACAMS scheme this is 20 points, but it could be any starting number), MEDIUM-RISK attributes have a score that is ½ of the HIGH-RISK score (i.e., 10 points), LOW-RISK attributes have a score that is ½ of the MEDIUM-RISK score (i.e., 5 points), and if a risk dimension is "Not Applicable" to a product whatsoever, the score is 0.
[NOTE: One could have started with any starting score for HIGH-RISK attributes AND applied the symmetry principle, and the results would remain the same. The application of this principle of symmetry represents a straightforward objective approach that avoids the subjective assignment of relative values.]

(3) **The application of that same principle of symmetry in the categorization of products/services as having Inherent HIGH, MEDIUM, and LOW ML Risk** – that is, with a maximum of 120 points potentially attributable to a product/service (20 points for high-risk attributes x 6 risk dimensions = 120 points), we divide that total into equal thirds. Thus, LOW-RISK sections are those with a score of 0 to 39, MEDIUM-RISK sections are those with a score between 40 and 79, and HIGH-RISK sections are those with a score of 80 to 120.

In the end, it is the test of reasonableness or common sense that judges the efficacy of this approach. ACAMS subjected the full range of financial products/services to the process described above, and process yielded entirely sensible results. That is, products/services one would expect to be identified as possessing high ML risk turned out HIGH RISK – for example, International Correspondent Banking, International Pouch Activity, Payable-through-Accounts, Private (aka High-Net-Worth) Banking, Remote Deposit Capture for Banks/Businesses, Trade Finance, International Bulk Shipments of Currency, Retail Money Transfer, Sale of Precious Metals/Coins. On the other hand, products/services one would expect to be of less attraction to money launderers (and thus less risk to financial institutions) end up being categorized as having LOW ML RISK – for example, Consumer Charge Cards, Term Deposits/CDs, Safety Deposit Boxes, Consumer and Business Travel Services, Student Loans, Payday Loans, Protective Insurance (Homeowner's, Vehicle, Renter's). [NOTE: ACAMS strongly believes that, while some products may possess LOW ML RISK, there is no such thing ZERO ML RISK.]

Several examples of the evaluation process for a product's inherent ML risk follow:

	Remote Deposit Capture (RDC) for Banks and Businesses	**International Bulk Shipment of Currency**	**Re-loadable Prepaid Access Products (Open System)**	**Student Loans**	**Insurance Products with Cash/ Surrender Value**
Risk Dimension 1 = Involves cash/ cash-based monetary instruments	(1c – LOW) Product/service may occasionally, but not characteristically, involve value transfer in currency.	(1a1 – HIGH) Core feature of product/service is that it actually involves currency itself	(1a2 – HIGH) Core feature of product/service involves value in bearer-negotiable form (such as pre-paid card of any type).	(1c – LOW) Product/service may occasionally, but not characteristically, involve value transfer in currency.	(1c – LOW) Product/service may occasionally, but not characteristically, involve value transfer in currency
Risk Dimension 2 = Supports anonymity	(2a2 – HIGH) Core feature of product/service is that there is little or no face-face interaction between customer/holder and the location where the product/service is being used	(2a3 – HIGH) Product/service can easily involve the concealment of beneficial ownership of funds/source of funds.	(2a1 – HIGH) Core feature of product/service is that it is anonymous = i.e., little or no identification of the customer/holder is involved with product/service's use.	(2d) Not Applicable -- i.e., anonymous acquisition and/or use of the product/service is not supported.	(2d) Not Applicable -- i.e., anonymous acquisition and/or use of the product/service is not supported.
Risk Dimension 3 = Involves rapid value transfer	(3b1 – MEDIUM) Product/service usually involves value transfer in near-term – i.e., within 1-3 days.	(3b – MEDIUM) Product/service usually involves value transfer in near-term – i.e., within 1-3 days.	(3b2 – MEDIUM) Core feature of the product/service is immediacy of negotiability + wide acceptance.	(3b2 – MEDIUM) Core feature of the product/service is immediacy of negotiability + wide acceptance.	(3b – MEDIUM) Product/service usually involves value transfer in near-term – i.e., within 1-3 days.
Riske Dimension 4 = Involves large value transfer	(4a – HIGH) Product/service is NOT restrictive to easy transfer of large value	(4a – HIGH) Product/service is NOT restrictive to easy transfer of large value	(4a – HIGH) Product/service is NOT restrictive to easy transfer of large value	(4b – MEDIUM) Product/service has restrictions/limits on value and frequency/timing that restrict transfers to less than $100,000 annually but > $25,000 annually.	(4a – HIGH) Product/service is NOT restrictive to easy transfer of large value
Risk Dimension 5 = Involves cross-border value	(5c – LOW) Although NOT a core feature of the product/service, it can allow possible	(5a – HIGH) Core feature of product/service is that it involves	(5c – LOW) Although NOT a core feature of the product/service, it can allow possible cross-	(5c – LOW) Although NOT a core feature of the product/service, it	(5c – LOW) Although NOT a core feature of the product/service, it

transfer	cross-border transfer of value.	cross-border transfer of value – e.g., foreign wire transfers into/out of a country.	border transfer of value.	can allow possible cross-border transfer of value.	can allow possible cross-border transfer of value.
Risk Dimension 6 = Supports involvement of unrelated 3rd parties	(6a – HIGH) Core feature of Product/service involves nested/obscured relationships (e.g., customers of our clients).	(6d) Not Applicable -- i.e., product/service restricted to customer of record.	(6b2 – MEDIUM) Product/service use may involve 3rd parties unrelated to the customer (e.g., encashment, use for POS transactions, use for ATM withdrawal, etc.)	(6b1 – MEDIUM) Product/service funding may involve 3rd parties unrelated to the customer (e.g., via wire transfer, cash remittance, check)	(6b1 – MEDIUM) Product/service funding may involve 3rd parties unrelated to the customer (e.g., via wire transfer, cash remittance, check)
ML Risk Score Calculation	RD 1 = 5 RD2 = 20 RD3 = 10 RD4 = 20 RD5 = 5 RD6 = 20 Total score = 80	RD 1 = 20 RD2 = 20 RD3 = 10 RD4 = 20 RD5 = 20 RD6 = 0 Total score = 90	RD 1 = 20 RD2 = 20 RD3 = 10 RD4 = 20 RD5 = 5 RD6 = 10 Total score = 85	RD 1 = 5 RD2 = 0 RD3 = 10 RD4 = 10 RD5 = 5 RD6 = 10 Total score = 40	RD 1 = 5 RD2 = 0 RD3 = 10 RD4 = 20 RD5 = 5 RD6 = 10 Total score = 50
Inherent Risk Category	**HIGH**	**HIGH**	**HIGH**	**MEDIUM**	**MEDIUM**

Scoring a Product's Incidental Features

ACAMS made the distinction between a product's core features (that are intrinsic to that product's nature) and its incidental features (that may potentially but not necessarily be used by the product's owner/user). The ACAMS perspective on a product's incidental features is that financial institutions are just as answerable for the mitigation of the ML risks such features pose as they are for the product's core features.

For example, a Demand Deposit Account's core feature vis-à-vis anonymity is that it is issued to a known individual. This would yield a score of "0" for the Risk Dimension of "Supports Anonymity." However, a DDA can potentially be accessed by an anonymous individual who has been given a debit card and PIN. A financial institution should have controls in place to mitigate the risk of such possible situations. Similarly, Consumer Charge or Credit Cards have a small likelihood of involving cross-border value transfer (and thus the score for that Risk Dimension would be LOW or a score of "5"). However, significant cross-border value transfer can potentially occur through either payments made on debt from abroad and/or through ATM withdrawals made overseas. The risk of these two potential transactions involving Credit/Charge Cards raises the score for that Risk Dimension to "20", and financial institutions offering such products would be expected to have internal preventative and detective controls in place to mitigate that risk.

Thus, a product's incidental features may have the effect of increasing the score of a particular risk dimension. [NOTE: A risk dimension's score can be raised to no more than the maximum of 20 points.]

Mitigating a Product's Features through Internal Preventative and Detective Controls

The essence of the ACAMS Risk Assessment system is that, for all the core and incidental features relevant to ML risk for all the products/services offered by a financial institution, ACAMS will lead the user through questions on the application of risk mitigation controls. These measures are organized under the headings of "Preventative Controls" (PCs = policies/procedures, terms and conditions, prohibitions, limits, etc., aimed at eliminating or mitigating risk) and "Detective Controls" (DCs = reporting and monitoring systems and associated business rules aimed at highlighting unusual activity that deserves an explanation and may be suspicious and reportable to government authorities). ACAMS has done extensive research and consulted its Committee of Experts to identify the key PCs and DCs associated with the risk mitigation of each risk dimension for each product.

Implementation of PCs and/or DCs has the effect of decreasing the score of a particular risk dimension. [NOTE: PCs and DCs cannot lower a risk dimension's score to less than "0".]

Derivation of a Product's Residual ML Risk

The following components interplay with one another in the ACAMS RA system to provide users with valuable information regarding their Product ML risk:

- A Financial Institution's products and services = a fixed starting point;
- The core features and inherent ML risk of those products associated with the six ML risk dimensions = a starting score that may be increased by . . .
- Possible incidental features associated with the six risk dimensions = additions to the inherent risk score that may yield an enhanced starting score;
- Internal preventative controls = potential subtractions from the starting (or enhanced starting) score;
- Internal detective controls = further potential subtractions from the starting (or enhanced starting) score;
- A product's residual risk score for each risk dimension;
- The final cumulative residual risk for a product.

The formula behind the calculation can be represented as:

Product RR = [RD1E – (RD1PC + RD1DC)] +
[RD2E – (RD2PC + RD2DC)] +
[RD3E – (RD3PC + RD3DC)] +
[RD4E – (RD4PC + RD4DC)] +
[RD5E – (RD5PC + RD5DC)] +
[RD6E – (RD6PC + RD6DC)]

Key
Product RR = Final Residual Risk for Product
RD1E = Enhanced Feature Risk for Risk Dimension 1
RD1PC = Preventative Control for Risk Dimension 1
RD1DC = Detective Control for Risk Dimension 1
.
.
.
RD6E = Enhanced Feature Risk for Risk Dimension 6
RD6PC = Preventative Control for Risk Dimension 6

Thus, at the end of the evaluation of product ML risk, users will gain insight into the status of the residual risk not only associated with each risk dimension but also for each product overall. Opportunities for improvement, if any are indicated, will be apparent from both a preventative and detective standpoint.

Appendix 2 – Customer/Entity Type AML Risk Tool Details

- Prohibited and High-Risk Customer Relationships
- Inherent Customer/Entity Risk Scoring
- Effect of Internal Preventative and Detective Controls
- Final Customer Type Residual Risk Calculation

Prohibited and High-Risk Customer Relationships

The ACAMS Customer/Entity ML Risk Assessment is relatively straightforward compared to the Product ML Risk Assessment. The process is based on the concepts of PROHIBITED and HIGH-RISK relationships with individual customers and business structure/industry customer types. These relationships are classified into the following general categories:

- **Prohibited individual customer/customer types designated by authoritative sources** = chiefly confirmed matches with official government sanctions lists;
- **Prohibited individual customer/customer types designated by Board-approved policy** = primarily undesirable customers with whom the institution has officially determined that it does not wish to do business;
- **Prohibited structure/industry/business customer types designated by authoritative sources** = includes confirmed matches with official government sanctions lists plus such entities as shell banks and bearer-share corporations;
- **Prohibited structure/industry/business customer types designated by Board-approved policy** = primarily undesirable types of business customers with which the institution has determined that it does not wish to have relationships;
- **Domestic PEPs** (politically exposed persons and their close associates), a group of individuals considered high-risk relationships;
- **Foreign PEPs** (politically exposed persons and their close associates), a group of individuals considered high-risk relationships;
- **Non-resident aliens**, a group of individuals considered high-risk relationships;
- **Other high-risk individual customer types designated by Board-approved policy**;
- **An extensive list of high-risk structure/industry/business customer types, designated either by authoritative sources or by Board-approved policy**, including such categories as:
    - Cash-intensive businesses;
    - Gaming and gambling establishments;
    - Vehicle dealerships;
    - Money service businesses – such as currency exchanges/casas de cambio, money transmitters, issuers of traveler's checks and money orders, check cashers, etc.;
    - Trusts;

- Dealers in high-value luxury goods;
- Real estate businesses;
- Specialized financial intermediaries;
- Professional service providers such as lawyers and accountants.

Inherent Risk Score for Above Prohibited and High-Risk Categories

The starting inherent risk score for each of these categories is 120 points, the same score as the maximum risk score for any of the products a financial institution may offer. ACAMS adopted this starting score based on the principle that the risk associated with any of these non-product categories, when unmitigated by an internal preventative and detective controls, would represent the same danger to a financial institution as their offering a maximum risk product without any mitigating controls.

For PROHIBITED customers/customer types, ACAMS assumes that the possibility exists that such customers may try to establish a relationship with a financial institution. Therefore, the RA Tool automatically starts with the maximum 120 points and follows with questions about appropriate internal controls.

For HIGH-RISK customers/customer types, ACAMS asks first whether or not such relationships actually exist. If the user answers "YES" to this question, then the RA Tool starts with the maximum 120 points and follows with questions about appropriate internal controls.

If the user answers "NO" to the question about existing relationships with any or all of the high-risk customer types, the RA tool next asks whether or not such relationships could potentially exist with the financial institution – for example, no domestic or foreign PEPs may currently have relationships BUT there are no conditions that would prevent such relationships in the future. If the user answers "YES" to this question, then the RA Tool starts with the maximum 120 points and follows with questions about appropriate internal controls.

On the other hand, if the user answers "NO" to both of the above questions (on existing or potential relationships with a high-risk type of customer), then the RA Tool requires the user to document via the narrative or via an attachment, how the relationship could not even potentially exist. The line of questioning outlined above related to internal controls is then terminated (i.e., no questions about internal questions are pursued) and the result is the automatic assignment of N/A (not applicable) for that category.

The Effect of Internal Preventative and Detective Controls

For all situations, except those involving no existing or potential relationships with high-risk customer types, the RA Tool launches a series of questions about internal preventative and detective controls that the user may have implemented to mitigate the risk. The existence of appropriate internal preventative controls may deduct a maximum of 60 points from the 120 point starting score. Likewise, the existence of appropriate internal detective controls may deduct a maximum of 60 points from the 120 point starting score.

Derivation of a Customer Type's Residual ML Risk

The following components interplay with one another in the ACAMS RA system to provide users with valuable information regarding their Customer Type ML risk:

- Prohibited Individual and Business Type Customers = a fixed starting score of 120 points;
- High-Risk Individual Customers/Customer Types with which a user has existing relationships OR has the potential to have such relationships = a fixed starting score of 120 points;
- High-Risk Business Customers/Customer Types with which a user has existing relationships OR has the potential to have such relationships = a fixed starting score of 120 points;
- High-Risk Individual or Business Customer Types with which the user has no existing relationships AND no potential for such relationships = no fixed points and the attribution of "N/A";
- Internal preventative controls = potential subtraction of a maximum of 60 points from the starting score;
- Internal detective controls = further potential subtraction of a maximum of 60 additional points from the starting score;
- The final residual risk for a Customer Type.

The formula behind the calculation can be represented as:

Cust RR = [120 – (PC + DC)]

Key
Cust RR = Final Residual Risk for a Customer Type
PC = Preventative Control for Customer Type
DC = Detective Control for Customer Type

Thus, at the end of the evaluation of Customer Type ML risk, users will gain insight into the status of the residual risk not only associated with each Individual and Business Customer Type but also overall Customer Type Risk. Opportunities for improvement, if any are indicated, will be apparent from both a preventative and detective standpoint.

Appendix 3 – Geographic AML Risk Tool Details

- Prohibited and High-Risk Geographies
- Inherent Geography Risk Scoring
- Effect of Internal Preventative and Detective Controls
- Final Geography Residual Risk Calculation

Relationships Involving Prohibited and High-Risk Geographies

The foreign jurisdictions with which a financial institution may be involved in some way can be major determinants of that financial institution's ML risk profile. The following list details some of the important ways in which a foreign jurisdiction may impact on a financial institution:

- The FI may have customers with home and/or mailing addresses in a jurisdiction;
- The FI may have customers whose source(s) of funds are in/from a jurisdiction;
- The FI may have customers who are citizens of a jurisdiction;
- The FI itself may be doing business in or with a jurisdiction;
- The FI's customers may be doing business in or with a jurisdiction, involving activities and/or transactions that require the FI's participation [Note: The FI would not necessarily have knowledge about every aspect of a customer's foreign finances and relationships.];
- The FI may, as an Ordering, Beneficiary, or Intermediary Institution, be handling electronic funds transfers involving a jurisdiction;
- The FI may be processing monetary instruments involving a jurisdiction;
- The FI, in some role in Trade Finance or a Letter of Credit, may become involved with a jurisdiction.

In the same manner as the ACAMS Customer Type ML Risk Assessment tool, the ACAMS Geographic ML Risk Assessment tool is based on the concepts of PROHIBITED and HIGH-RISK relationships, this time involving prohibited and high-risk geographies. These geographies are classified into the following general categories:

- **Prohibited foreign geographies** = those identified by OFAC, US Treasury, the UK Government, and other authoritative government agencies;
- **High-Risk Foreign Geographies** = foreign jurisdictions stipulated as high-risk by authoritative sources or determined by a financial institution's own policy;
- **High-Risk Domestic Geographies** = in the US, these are High-Intensity Financial Crime Areas (HIFCAs) and High-Intensity Drug Trafficking Areas (HIDTAs).

Inherent Risk Score for Above Prohibited and High-Risk Categories

The starting inherent risk score for these categories is 120 points, the same score as the maximum risk score for any of the products a financial institution may offer. ACAMS adopted this starting score based on the principle that the risk associated with these geographic categories, when unmitigated by an internal preventative and detective controls, would represent the same danger to a financial institution as their offering a maximum risk product without any mitigating controls.

For PROHIBITED geographies, ACAMS assumes that the possibility exists that relationships with such jurisdictions can occur or may be attempted with a financial institution at any time. Therefore, the RA Tool automatically starts with the maximum 120 points and follows with questions about appropriate internal controls.

For HIGH-RISK domestic and foreign geographies, ACAMS asks first whether or not such relationships actually exist. If the user answers "YES" to this question, then the RA Tool starts with the maximum 120 points and follows with questions about appropriate internal controls.

If the user answers "NO" to the question about existing relationships with high-risk domestic or foreign geographies, the RA tool next asks whether or not such relationships could potentially exist with the financial institution – for example, the FI may currently have no relationships involving Indonesia or Venezuela BUT there are no conditions that would prevent such relationships in the future. If the user answers "YES" to this question, then the RA Tool starts with the maximum 120 points and follows with questions about appropriate internal controls.

On the other hand, if the user answers "NO" to both of the above questions (on existing or potential relationships with a high-risk foreign geography), then the RA Tool terminates that line of questioning (i.e., no questions about internal questions are pursued), the Tool requires the user to document via the narrative or via an attachment how the relationship could not even potentially exist, and the result is the automatic assignment of N/A (not applicable) for that category.

The Effect of Internal Preventative and Detective Controls

For all situations, except those involving no existing or potential relationships with high-risk foreign or domestic geographies, the RA Tool launches a series of questions about internal preventative and detective controls that the user may have implemented to mitigate the risk. The existence of appropriate internal preventative controls may deduct a maximum of 60 points from the 120-point starting score. Likewise, the existence of appropriate internal detective controls may deduct a maximum of 60 points from the 120-point starting score.

Derivation of a Geography's Residual ML Risk

The following components interplay with one another in the ACAMS RA system to provide users with valuable information regarding their Geographic ML risk:

- Prohibited Foreign Geographies = a fixed starting score of 120 points;
- High-Risk Foreign Geographies with which a user has existing relationships OR has the potential to have such relationships = a fixed starting score of 120 points;
- High-Risk Domestic Geographies with which a user has existing relationships OR has the potential to have such relationships = a fixed starting score of 120 points;
- High-Risk Foreign and Domestic Geographies with which the user has no existing relationships AND no potential for such relationships = no fixed points and the attribution of "N/A";
- Internal preventative controls = potential subtraction of a maximum of 60 points from the starting score;
- Internal detective controls = further potential subtraction of a maximum of 60 additional points from the starting score;
- The final residual risk for a jurisdiction.

The formula behind the calculation can be represented as:

Geog RR = [120 – (PC + DC)]

Or

DomGeog RR = [120 — (PC+DC)]

Key
Geog RR = Final Residual Risk for a Geography
DomGeog RR = Final Residual Risk for Domestic High-Risk Geography
PC = Preventative Control for Geography
DC = Detective Control for Geography

Thus, at the end of the evaluation of Geographic ML risk, users will gain insight into the status of the residual risk not only associated with each Foreign and Domestic Geography but also overall Geographic Risk. Opportunities for improvement, if any are indicated, will be apparent from both a preventative and detective standpoint.

Appendix 4 - Guidance on Determining Strength of Controls based on Standardized AML Control Factor Evaluation

Current Tool Assessment of Strength of Controls

The current strength of control factors that the Tool considers may be used to determine the effectiveness of an institution's AML program controls and are as follows:

- Management oversight and accountability;
- Policies and procedures;
- Compliance training;
- Systems and operations;
- Business unit monitoring and QA;
- Regulatory environment;
- Personnel risk;
- Independent testing;
- Audits/reviews.

The Tool asks questions about but does not currently utilize user's answers about the strength of these controls in automatically influencing the final residual risk for products/services, customer types, or geographies. The guidance below has the objective to provide users with a practical, standardized approach to evaluate the strength of their controls.

Examples of control strength

Below are examples of how we suggest users distinguish among Weak (Ineffective), Moderate (Need Improvement), and Strong (Effective) Controls.

Distinguished are Preventative Controls (PCs = policies, procedures, limits, prohibitions, hold periods, etc.) and Detective Controls (DCs = audit assessments, monitoring rules, report reviews, other detection means, etc.).

Examples of weak controls (I.e., existing BUT ineffective)

- For DCs = "Business rules in concept only – not yet tested/implemented."
- For DCs = "Automated monitoring system/software being acquired – not yet tested/implemented. No other monitoring coverage in place."
- For DCs = "Manual monitoring process of report reviews in place but process is newly established and staff not fully trained."

- For DCs = “Monitoring business rules in production but never reviewed or optimized using standardized process.”
- For PCs = “Policy recently approved – procedures are in the process of being developed.”
- For PCs and/or DCs = “Staffing minimal – staffing adequacy not evaluated.”

Examples of moderate controls (I.e. existing BUT need improvement)

- For DCs = “Business rules in pilot/pre-production mode – currently being tested.”
- For DCs = “Business rules in production mode – currently undergoing optimization.”
- For DCs = “Automated monitoring system/software being acquired – Manual monitoring currently in place.”
- For DCs = “Regular manual monitoring of reports in place for product not requiring automated monitoring. However, procedures recently established (< 1 year) and staff newly trained.”
- For DCs = “Business rules in production. However, they are only subject to informal review and optimization.”
- For PCs = “Policy recently approved – procedures have been developed and staff are currently being trained.”
- For PCs and/or DCs = “Staffing appears substantial – however, staffing adequacy not formally evaluated.”
- For PCs and/or DCs = “Staffing being actively increased – staff being recruited/interviewed based on formal evaluation.”

Examples of strong controls (I.e. Effective)

- For DCs = “Business rules in production after having been optimized with a formal parameter optimization process.”
- For DCs = “Automated monitoring system in production. Former manual process decommissioned.”
- For DCs = “Regular manual monitoring of reports in place for product not requiring automated monitoring. Procedures fully established (> 1 year) and staff fully trained.”

- For DCs = “Business rules in production. Formal annual review process in place.”
- For PCs = “ Policy approved – staff fully trained in related procedures”
- For PCs and/or DCs = “Staffing optimal – based on formal evaluation of staffing requirements.”
- For PCs and/or DCs = “Independent review (by Internal Audit, Regulatory Examination, and/or External Audit) has found the controls adequate.”

Method for Scoring PC and DC Strength of Controls:

This solution is based on the current 9 control factors and it relies on a “rounding” process that accommodates the use of values at multiples of “0.5.”

Scoring for Strength of Controls Related to Products Assumptions

(1) The maximum score for a Product is 120 points, assuming that the Inherent Risk (that is, the Inherent Risk + Feature Risk) for each of the 6 Risk Dimensions is 20 points.

(2) The actual Inherent Risk for each of the 6 Risk Dimensions can be either 0 points, 5 points, 10 points, or 20 points.

(3) Therefore, the actual possible points for Preventative and Detective Controls is either 0, 2.5 points, 5 points, or 10 points.

(4) The current RA Tool limits reductions in points for the implementation of PCs and DCs to multiples of “0.5”, including the assessment of strength of controls.

(5) A “rounding” process has been introduced whereby all formula results involving the assessment of strength of controls are rounded to the nearest “0.5” in order to accommodate the above limitation.

Scoring Approach for each of a Product’s Risk Dimensions

Depending on what the Inherent Risk score is for a Product’s Risk Dimension, the related PCs and DCs may be worth a maximum deduction of -2.5 points, -5 points, or -10 points. The strength of a PC or DC is currently based on 9 strength of control factors.

To set up the formula:

- If $Control_n$ = Effective, then $Deduction_n$ **= -(1/9 x 1) = -0.11**

- If Control$_n$ = Needs Improvement, then Deduction$_n$ = **-(1/9 x 0.5) = -0.056**

- If Control$_n$ = Weak/Ineffective, then Deduction$_n$ = **-(1/9 x 0) = -0**

And the resultant formula for a PC or DC valued at 10 points would be:

- [Control$_1$strength(Deduction$_1$) + Control$_2$strength(Deduction$_2$) + Control$_3$strength(Deduction$_3$) + Control$_4$strength(Deduction$_4$) + Control$_5$strength(Deduction$_5$) + Control$_6$strength(Deduction$_6$) + Control$_7$strength(Deduction$_7$) + Control$_8$strength(Deduction$_8$) + Control$_9$strength(Deduction$_9$)] = "X" x 10 = **Final Deduction**

And the resultant formula for a PC or DC valued at 5 points would be:

- [Control$_1$strength(Deduction$_1$) + Control$_2$strength(Deduction$_2$) + Control$_3$strength(Deduction$_3$) + Control$_4$strength(Deduction$_4$) + Control$_5$strength(Deduction$_5$) + Control$_6$strength(Deduction$_6$) + Control$_7$strength(Deduction$_7$) + Control$_8$strength(Deduction$_8$) + Control$_9$strength(Deduction$_9$)] = "X" x 5 = **Final Deduction**

And the resultant formula for a PC or DC valued at 2.5 points would be:

- [Control$_1$strength(Deduction$_1$) + Control$_2$strength(Deduction$_2$) + Control$_3$strength(Deduction$_3$) + Control$_4$strength(Deduction$_4$) + Control$_5$strength(Deduction$_5$) + Control$_6$strength(Deduction$_6$) + Control$_7$strength(Deduction$_7$) + Control$_8$strength(Deduction$_8$) + Control$_9$strength(Deduction$_9$)]= "X" x 2.5 = **Final Deduction**

Some examples should help clarify the use of the above formulas:

Example #1 in which the following assessments of Controls 1-9 exists = Control$_1$strength = effective; Control$_2$strength = effective; Control$_3$strength = effective; Control$_4$strength = Needs improvement; Control$_5$strength = Needs improvement;
Control$_6$strength = Needs improvement; Control$_7$strength = Needs improvement; Control$_8$strength = Needs improvement; Control$_9$strength = Ineffective.

- For PC or DC worth 10 points -> (1/9x1) + (1/9x1) + (1/9x 1) + (1/9x 0.5) + (1/9x 0.5) + (1/9x 0.5) + (1/9x 0.5) + (1/9x .05) + (1/9x 0) = .11 + .11 + .11 + .056 + .056 + .056 + .056 + .056 + 0 = 0.61 x 10 points = **-6.1 points (rounded to -6.0)**

- For PC or DC worth 5 points -> (1/9x1) + (1/9x1) + (1/9x 1) + (1/9x 0.5) + (1/9x 0.5) + (1/9x 0.5) + (1/9x 0.5) + (1/9x .05) + (1/9x 0) = .11 + .11 + .11 + .056 + .056 + .056 + .056 + .056 + 0 = 0.61 x 5 points = **-3.05 points (rounded to -3.0)**

- For PC or DC worth 2.5 points -> (1/9x1) + (1/9x1) + (1/9x 1) + (1/9x 0.5) + (1/9x 0.5) + (1/9x 0.5) + (1/9x 0.5) + (1/9x .05) + (1/9x 0) = .11 + .11 + .11 + .056 + .056 + .056 + .056 + .056 + 0 = 0.61 x 2.5 points = **-1.525 points (rounded to -1.5)**

Example #2 in which the following assessments of Controls 1-9 exists = Control$_1$strength = effective; Control$_2$strength = effective; Control$_3$strength = ineffective; Control$_4$strength = ineffective;

Control$_5$strength = ineffective; Control$_6$strength = ineffective; Control$_7$strength = ineffective; Control$_8$strength = ineffective; Control$_9$strength = ineffective.

- For PC or DC worth 10 points -> (1/9x1) + (1/9x1) + (1/9x 0) + (1/9x 0) + (1/9x 0) + (1/9x 0) + (1/9x 0) + (1/9x .0) + (1/9x 0) = .11 + .11 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0.22 x 10 points = **-2.2 points (rounded to -2.0)**

- For PC or DC worth 5 points -> (1/9x1) + (1/9x1) + (1/9x 0) + (1/9x 0) + (1/9x 0) + (1/9x 0) + (1/9x 0) + (1/9x .0) + (1/9x 0) = .11 + .11 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0.22 x 5 points = **-1.1 points (rounded to -1.0)**

- For PC or DC worth 2.5 points -> (1/9x1) + (1/9x1) + (1/9x 0) + (1/9x 0) + (1/9x 0) + (1/9x 0) + (1/9x 0) + (1/9x .0) + (1/9x 0) = .11 + .11 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0.22 x 2.5 points = **-0.55 points (rounded to -0.5)**

Final Residual Risk for a Product

Once the final deduction for each of the 6 risk dimensions is calculated, a final Residual Risk score for a Product results.

For example, if the **Inherent Risk of a Product** (aggregated for all 6 risk dimensions) is **90 points**, AND the **deductions for PC and DC controls** (including the assessment of the strength of those controls per above formulas) is **-55.50 points**, the Residual Risk for that Product = **34.5 points**, which would be deemed **LOW**.

Appendix 5 - AML Risk Tool Development, Oversight and Maintenance

- AML Risk Tool Development
- AML Risk Tool Oversight
- Annual AML Risk Tool Review/Maintenance
- Ad Hoc AML Risk Tool Review/Maintenance

AML Risk Tool Development

The ACAMS risk tool development process includes:

- ACAMS assumes responsibility for all the risk components used in the RA Tool.
- At a minimum, ACAMS will review all tool components on an annual basis. However, if circumstances warrant, tool components may be updated on an ad hoc basis.
- ACAMS will consult on proposed methodology changes with its subject matter experts.
- The ACAMS will create a user group and feedback mechanism, whereby input and suggestions on the RA Tool and methodology.

AML Risk Tool Oversight

Tool oversight includes:

- Tanya Montoya (Director of Product Management – AML Risk) will have oversight of the tool and its components.
- ACAMS may engage the services of an experienced subject matter expert to assist in product oversight.

Annual AML Risk Tool Review/Maintenance

Annual tool review and maintenance will involve:

- At a minimum, ACAMS will review the tool and its components and may, depending on findings as well as feedback from the users group, decide to evaluate changes in the tool.
- Any changes that are contemplated will be thoroughly evaluated as far as their potential impact and development costs.
- ACAMS will consult on proposed tool changes with its subject matter experts.
- Changes approved by ACAMS executives will go through the full software development cycle of preliminary testing and beta testing before production.

Ad Hoc AML Risk Tool Review/Maintenance

The ACAMS AML Risk Tool and its components may also be updated as information becomes available that impacts the factors used to evaluate the potential risks. Circumstances that may lead to changes in the tool on an ad hoc basis include:

- Completely new financial products and services may be developed that are required to be added to the Product AML Risk Tool;
- Governments may change laws and regulations related to money laundering and terrorist financing;
- Authorities may designate additional foreign jurisdictions as prohibited and/or may remove jurisdictions from such designation;
- Authorities may update their guidance on the ML risk associated with certain financial products;
- Authorities may issue new guidance on high-risk types of individual and business customers;
- Changes in economic or political conditions may occur that necessitate consideration of changes in the risk tool.

When any of the above circumstances arise, a review of the affected Risk Tool components will be undertaken to determine IF changes are warranted.

As with the annual maintenance:

- Any changes that are contemplated will be thoroughly evaluated as far as their potential impact and development costs;
- That ACAMS will consult on proposed methodology changes with its subject matter expert.
- Changes approved by ACAMS executives will go through the full software development cycle of preliminary testing and beta testing before production.

Questions?

Should you have any questions related to the ACAMS Risk Assessment methodology, please contact Tanya Montoya, ACAMS Director of Product Management, via email at tmontoya@acamsra.com.