CREATING AN EFFECTIVE AML AUDIT / REVIEW PROGRAM

Anti-money laundering (AML) audits and reviews are one of the best ways to reveal whether your AML systems and control program are working, and where it might fall short. Achieving these goals can be a challenge due to the complexities of conducting the audit review itself. This session will provide guidance for managing this function. From assessing regulatory expectations, to assembling the right technology and expertise, and interpreting the results to improve your compliance regime, this session provides workable solutions to seemingly difficult issues.

DERRICK CERNA, CFE, CAMS, LLM
Senior Director
Mizuho Bank
London

Following his NYU graduation Rick Cerna relocated to Los Angeles where he joined the legal department of Metro-Goldwyn-Mayer Studios focusing on sale-leaseback agreements, contracts, and corporate financing. Later, Cerna joined the London office of the New York law firm Cleary, Gottlieb, Steen & Hamilton with a focus on IPO's, regulatory and corporate work. Cerna continued his career by joining the Los Angeles office of the law firm Skadden, Arps. After Cerna returned to New York in 2011, he worked in the legal department of Citco Fund Services, the largest hedge fund administrators in the world. In 2013, he took oversight of the Citco Due Diligence Group working under the Compliance / AML umbrella of the firm. Cerna later returned to London, joining J.P. Morgan Chase as a Vice President of the KYC Remediation Team, acting as a case lead on policy implementation re foreign correspondent banking, corporates, and NBFIs in the EMEA region (with a specific concentration on France).

In December 2015, Mr. Cerna joined Mizuho Bank, Ltd. as a senior director and head of the AML Enhancement Team. He oversees a team of AML specialists who travel throughout EMEA and review branches and subsidiaries of Mizuho in order to standardise the JMOF, OFAC and local regulatory policies and procedures of each. Ensuring that transaction monitoring detection rules, sanctions, and KYC procedures are robust is another facet of the team's responsibilities. A risk-based approach is highlighted as a theme of this coverage.

“Association of Certified Fraud Examiners,” “Certified Fraud Examiner,” “CFE,” “ACFE,” and the ACFE Logo are trademarks owned by the Association of Certified Fraud Examiners, Inc. The contents of this paper may not be transmitted, republished, modified, reproduced, distributed, copied, or sold without the prior consent of the author.
PLEASE NOTE: The views expressed in this paper are those of the author, and the author alone. The author is not necessarily representing the views of Mizuho Bank, Ltd. or any of its affiliates.

To successfully hike and navigate a day trail in a forest or mountainous area where you have never been before requires preparation and having the right tools. (Boots, water canteen/bottles, flashlight, matches/fire starter, hat, first-aid kit, compass/map, sunscreen, lip balm, knife/multi-tool, extra day food supply, whistle, emergency shelter, trekking poles, insect repellent, 2-way radio, multi-function watch, personal locator beacon, satellite phone, sunglasses—tools that act collectively as a survival kit.)

The primary objective of this discussion is to offer specific considerations and suggestions for how a financial institution’s (FI’s) internal audit department or AML Monitoring or Enhancement Team (Audit) can design a firm-wide AML risk assessment procedure that:
1. Assists the auditor’s in identifying AML risks;
2. Establishes the basis for thoughtful and supported risk determinations; and
3. Creates results that can help an audit plan to satisfy current regulatory expectations.

Overview

Regulatory Expectations Have Changed
Within the past five years, the financial services industry has experienced noticeable changes in regulatory expectations regarding the adequacy and overall view of internal controls. There has also been an increase in the frequency and severity of enforcement actions among the world’s largest and most reputable financial corporations.
Below are a few frequently cited AML program weaknesses:
- Inadequate customer due diligence and enhanced due diligence practices
- Incomplete identification of high-risk customers
- Insufficient policies, procedures, and training
- Failures in monitoring and identifying suspicious activity
- Poor reporting and filing practices related to suspicious activity
- Ineffective independent testing and audit functions

The expectation is for FIs to be less reactive and more proactive (e.g., by enhancing their risk management practices and strengthening their audit regime) has become a minimum standard in the eyes of supervisory agencies. This includes further attention to:
- A risk-based approach
- Timely identification of deviations
- Testing the adequacy

**The Audit Plan versus Regulator Expectations**
Audit should assemble a plan that demonstrates its organization’s knowledge of its Business Units (for the purposes herein, all business areas, control functions/utilities, and Lines of Businesses ([LOBs]) will be referred to collectively as Business Units), and an understanding of the business’s associated risks.

**The Risk Assessment Process**
An audit plan that includes every possible auditable Business Unit is arguably not a “plan” and is an unrealistic approach. A successful risk assessment should result in a detailed risk profile for each Business Unit, which can subsequently drive the level of audit coverage, including both scope (e.g., extent of testing
areas/testing steps) and frequency (e.g., annually, bi-annually).

**AML Risk Assessment Audit versus Other AML Risk Assessments**
There are different risk assessment methodologies, and these can be based on the FI/department that the tool is designed for and how the results will ultimately be used. The predominant objective of an AMLRA is to identify and assess potential risk (e.g., control gaps) in order to create an AML risk assessment that can pinpoint areas warranting immediate escalation (such as a blatant difference in how Audit has perceived a risk versus the business line’s view) or areas warranting further testing. Audit might also risk rate control gaps and weakness to assist the business with planning its activities.

**The Risk Assessment Tool**

**Overview**
Based on the Federal Financial Institutions Examination Council (FFIEC) and other leading industry sources, there are certain categories of inherent AML risk that apply broadly across the financial industry and are universally accepted as standard risks that must be addressed.

Primary inherent AML risks that relate broadly to an FI include:
1. Customers
2. Products and services
3. Transaction activity
4. Geographic presence

Pursuant to an FI's obligation to maintain an adequate AML compliance program, FIs are expected to
establish a control environment that minimizes AML risks. When evaluating a Business Unit's control environment, the audit department should assess the current state relating to:

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

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

**Inherent Risks**

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

- **Customers**
  
  Certain customers might pose a higher risk of money laundering and/or terrorist financing with respect to unique characteristics, such as the nature of their business (for legal entities), their occupation (for individuals), the duration of the relationship with the FI, and/or the number of accounts across various business lines.
Potential considerations for assessing the level of risk (i.e., high, medium, low) include:

**HR CUSTOMER TYPES**
This commonly includes particular industries/occupations (e.g., small arms manufacturing, used car dealers) or other designated customer categories that might require special due diligence (e.g., nongovernmental organizations, bearer share entities, money services businesses and foreign exchange houses, third-party payment processors, politically exposed persons [PEPS]).

**DURATION OF RELATIONSHIP**
FIs tend to have a better understanding of their customers' expected behaviour when they have had time to observe them and interact with them.

**CLOSED/BLOCKED ACCOUNTS**
Bank-initiated account closures and/or account blocks might be indicative of customer characteristics or transactions that are questionable or undesirable.

**NUMBER AND NATURE OF ACCOUNTS**
Customers who have accounts or access to services across multiple Business Units, as well as customers with accounts that offer enhanced or flexible features (e.g., higher transactions limits, minimal restrictions), might present increased risk exposure due to their ability to conduct a wider range of activities such as those involving additional products and services, delivery channels, locations, or account types.
**Products and Services**

Certain products and services pose a higher risk of money laundering and/or terrorist financing depending on the nature of the products and services and the capacity in which they can be used. Particular products and services, for instance, can support a higher degree of anonymity (e.g., prepaid cards, Internet banking, virtual currency), allow for third-party engagement (e.g., remotely created checks [RCCs], U.S. dollar drafts), or facilitate the handling of high volumes of currency or currency equivalents across less regulated jurisdictions (e.g., cross-border wire transfers).

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

**HR PRODUCTS AND SERVICES**

This commonly includes particular products and services that are complex in nature or that offer the potential for anonymity, speed, or transferability (e.g., remote deposit capture [RDC], trade finance, payable-through accounts, prepaid cards, certain types of mobile technology).

**NEW PRODUCTS AND SERVICES**

A Business Unit with a greater number of new products and services might pose a higher risk than a Business Unit with more established and familiar products and services that have been previously evaluated, monitored, and/or used.

**Transaction Activity**

Certain transactional behaviour and patterns, such as a high volume of transactions, large aggregate dollar amounts of activity or transactions entering and leaving accounts at high speeds (also known as velocity), might
warrant further attention as money laundering and/or terrorist financing often involves transaction activity characterized by complex flows, higher speeds, and sometimes larger dollar amounts to obscure audit trails of select transactions and accumulate sufficient funds to support criminal intentions.

**DEGREE OF BUSINESS/SALES GENERATED FROM HR PRODUCTS AND SERVICES**
Although a Business Unit might not offer a significant number of HR products and services, this does not necessarily negate the risk of having a relatively high amount of revenue generated from the use of HR products and services.

**RISK TOLERANCE**
Business Units with a higher tolerance for risk are inherently more risky, regardless of the controls that might be in place.

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

**ACTIVITY INVOLVING HR PRODUCTS AND SERVICES**
A Business Unit with a high overall volume and/or dollar value of activity involving products and services that are considered to be HR by the Business Unit may pose higher risk than a Business Unit that reflects less activity involving HR products and services.

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

**REPORTABLE TRANSACTION ACTIVITY**
Transaction activity reports include suspicious transaction reports (STRs), suspicious activity reports (SARs), and other related reports such as currency transaction reports (CTRs).

**Geographic Presence**
An extensive amount of work has been performed by established and internationally recognized organizations (e.g., OFAC, Financial Crimes Enforcement Network [FinCEN], Financial Action Task Force [FATF], Transparency International) to evaluate and risk rate countries based on their capacity to foster money laundering. Available informational sources and lists include the FATF Black List; the Section 311 designated countries list; Specially Designated Nationals (SDN) and Blocked Persons List; countries subject to OFAC sanctions; offshore financial centres (OFC); high-intensity drug trafficking areas (HIDTA); high-intensity financial crime areas (HIFCA); as well as other non-U.S. lists.

Potential considerations for assessing the level of risk (i.e., high, medium, low) include:
CUSTOMERS IN HR LOCATIONS
A significant number of customers with a known presence in a HR location might pose increased money laundering and/or terrorist financing risk due to their ability to accumulate and route funds through less secure regions.

PHYSICAL PRESENCE IN HR LOCATIONS
The extent to which a Business Unit is involved with HR jurisdictions might, to some degree, be reflected by whether the Business Unit has access to a physical operating branch or legal entity within a HR jurisdiction.

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

Control Environment and Risk Mitigants
Potential control environment areas include, but are not limited to:

Know Your Customer (KYC)
This initial risk profile, which includes customer details such as identifying information (e.g., legal name, address, government identification number) and basic due diligence (e.g., customer type, anticipated activity, name screening results) is often used to risk rate the customer (i.e., high, medium, low) in accordance with the FI’s customer risk scoring methodology.
<table>
<thead>
<tr>
<th>CREATING AN EFFECTIVE AML AUDIT / REVIEW PROGRAM</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>KYC requirements and functions, including customer identification programs (CIP), customer due diligence (CDD), enhanced due diligence (EDD), and special circumstances due diligence should be clearly defined and aligned to customer attributes and risks.</td>
<td></td>
</tr>
<tr>
<td>Potential considerations for assessing the strength (i.e., strong, adequate, weak) of the control include:</td>
<td></td>
</tr>
<tr>
<td><strong>EXCEPTIONS OR WAIVERS</strong></td>
<td></td>
</tr>
<tr>
<td>Although deviations from agreed-upon practices might be reasonable in specific circumstances, a significant number of exceptions or waivers can pose additional challenges in maintaining adequate and consistent information and can weaken the control environment.</td>
<td></td>
</tr>
<tr>
<td><strong>COMPLETENESS OF CUSTOMER INFORMATION</strong></td>
<td></td>
</tr>
<tr>
<td>Customer profiles that lack the required KYC components fail to adequately represent the customer and can result in inaccurate risk ratings.</td>
<td></td>
</tr>
<tr>
<td><strong>RELIANCE</strong></td>
<td></td>
</tr>
<tr>
<td>Reliance on other Business Units or third parties to perform KYC processes or to provide customer information is at times appropriate. Extensive reliance can diminish the Business Unit's ability to demonstrate that it understands its customer.</td>
<td></td>
</tr>
<tr>
<td><strong>RENEWALS, UPDATES, AND PERIODIC REVIEWS</strong></td>
<td></td>
</tr>
<tr>
<td>Performing periodic risk-based renewals or rolling reviews and maintaining up-to-date customer information are critical components of understanding the customer base. This involves looking for changes in KYC information (e.g., expected account activity, employment or business</td>
<td></td>
</tr>
</tbody>
</table>
CREATING AN EFFECTIVE AML AUDIT / REVIEW PROGRAM

details, business ownership, etc.) as well as being cognizant of HR activity in low-risk accounts.

CUSTOMER NAME SCREENING
This function usually occurs at account opening and renewal stages and includes the identification of PEPs, customers who might appear in section 314(a) search requests, customers who are subjects of adverse information, or customers who appear on internal “bad guy” lists (e.g., customers with whom the FI might not want to conduct business). Policies and procedures should define material versus immaterial matches, articulate the screening process (including escalation or referral points), and clearly indicate expected screening requirements by customer type and related parties (e.g., beneficial owners, authorized signers, powers of attorney, persons with authority to influence the account or respective funds). Where automated screening mechanisms are employed, testing procedures should be documented and followed, and algorithms, such as fuzzy logic, should be supported (e.g., rationale for how threshold levels were selected).

Potentially Suspicious and/or Unusual Activity (PSUA)
FIs are expected to be vigilant and to establish formal methods for effectively evaluating customer activity, managing alerts, conducting investigations, and determining whether to file a SAR or a STR (non-U.S. suspicious transactions report). A robust control environment should include well-defined and effective processes for promptly detecting, monitoring, escalating, investigating, decision-making, and filing potentially suspicious and/or unusual activity (referred to collectively as “PSUA” for the purposes herein).
Potential considerations for assessing the strength (i.e., strong, adequate, weak) of the control include:

**DETECTION AND MONITORING**

FIIs have a number of channels for which to identify PSUA. At a high level, these include: activities conducted as part of normal operations (e.g., manual monitoring, such as activity observed and referred by employees); activities conducted as a result of law enforcement and government requests (e.g., subpoenas, national security letters, section 314(a) and 314(b) information sharing); and information obtained via surveillance monitoring systems. At a minimum, the following reports should be reliable, complete, and routinely available: currency activity reports, funds transfer reports, velocity of funds reports, wire transfer records, monetary instrument reports, large item reports, significant balance change reports, and nonsufficient funds reports. Automated monitoring mechanisms and related technology (e.g., commercial products such as Fiserv, Oracle, or SAS as well as in-house solutions) are often used to capture, monitor, and alert on PSUA on a continuous basis.

**SOURCE DATA AND INTERNAL REPORTS RELATING TO PSUA**

The ability to produce effective and timely reports that assist in identifying PSUA (e.g., manual MIS or surveillance monitoring reports) and that adhere to U.S. and non-U.S. reporting requirements is dependent on both the quality and completeness of the source data.
ESCALATION AND REFERRAL OF ACTIVITY
Policies, procedures, and processes should be in place for referring PSUA from all areas of the Business Unit to the personnel department or department responsible for evaluating PSUA. This includes establishing and documenting a clear and defined escalation process from the point of initial detection to the completion of the investigation.

INVESTIGATION
As a best practice, the process of investigating an alert and determining whether a SAR should be filed (often referred to as case management), should include clear decision-making and documentation standards. SAR documentation should be thorough and include the reason for filing (or the rationale for not filing), as well as additional considerations, such as whether to close an account as a result of continuous suspicious activity. Although the decision to file a SAR might be subjectively determined, Business Units should establish an effective investigative and SAR decision-making process.

SAR/STR COMPLETION AND FILING
Numerous SAR users, such as intelligence agencies, law enforcement, regulatory authorities, and FinCEN all rely on the details provided in SARs. Information provided by FIs is used to execute investigations, gather intelligence about emerging money laundering tactics, identify illegal activities, and prosecute criminals. Where a decision is made to file a SAR, the quality of the SAR content is critical to the effectiveness of the suspicious activity reporting system.
OFAC and Sanctions
OFAC regulations and other regional and international mandates (e.g., United Nations sanctions) include requirements to block accounts and other property or to prohibit or reject transactions with specific countries, entities, and individuals as appropriate. As stated in the FFIEC manual, “All U.S. persons must comply with OFAC regulations, including all citizens and permanent resident aliens regardless of where they are located, all persons and entities within the United States, all U.S. incorporated entities and their foreign branches. In the case of certain programs, such as those regarding Cuba and North Korea, foreign subsidiaries owned or controlled by U.S. companies also must comply.”

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

OFAC SCREENING AND PROCESSING
OFAC screening controls relate broadly to the functions associated with maintaining OFAC-related lists and identifying accounts or property that might need to be blocked or transactions that might need to be prohibited or rejected, such as those involving Burma, Cuba, Iran, Sudan and/or Syria. This includes, but is not limited to: checking accounts against OFAC lists prior to initial account opening (e.g., for non-customer transactions), or shortly thereafter; identifying and investigating potentially relevant transactions; managing blocked funds and accounts (e.g., status, amount, ownership details, interest, etc.); regularly testing filtering criteria for issues (e.g., misspellings and name derivations); developing and adjusting parameters as appropriate to account for known risks (e.g., false positives, truncated payment
instructions, incorrectly coded or characterized transactions, “cover payments,” “straight-through processing”).

OFAC POLICIES AND PROCEDURES
Policies and procedures should address all aspects of OFAC compliance and controls, including customer onboarding, screening, and transaction review processes; management of blocked accounts; recordkeeping requirements; maintaining OFAC licenses; independent testing functions; roles and responsibilities for OFAC compliance; open lines of communication; specialized training; and reporting requirements.

OFAC LICENSES
Subject to specific provisions and clearly documented conditions, OFAC licenses allow for certain exceptions to OFAC requirements for select transactions that are deemed to be in line with U.S. policy objectives. In addition, OFAC may grant a general license that applies to a group or a category of transactions without requiring one-off approvals from OFAC.

OFAC REPORTING AND RELATED METRICS
In accordance with OFAC regulations, the Business Unit is required to report all blocked payments to OFAC within ten days of the occurrence and annually by September 30; once those assets or funds are blocked, they are to be placed in a blocked account. Prohibited transactions that are rejected must also be reported to OFAC within ten days of the occurrence.
Employee AML Expertise and Coverage

Regulatory bodies, such as the Office of the Comptroller Currency (OCC), have highlighted this message by alluding to inadequate staffing as a root cause for compliance failures in several enforcement actions. In order to prevent staff-related issues and minimize the risk of human error, AML functions and responsibilities should, at a minimum, encompass an adequate number of resources, a sufficient level of aggregate AML expertise among the staff, and an appropriate allocation of time to AML tasks by seasoned personnel.

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

AML STAFFING COVERAGE
A Business Unit should be able to demonstrate that it has a staffing plan or strategy in place to account for proper AML coverage—particularly in HR areas. This includes, but is not limited to, a focus on: (a) total number of available resources; (b) AML competency among those resources; and (c) distribution of time and effort among the pool of available AML resources.

EMPLOYEE KNOWLEDGE AND CAPABILITIES
Relevant indicators of expertise include: (a) the extent of technical knowledge over the tools and systems that are required for the relevant job function(s); (b) the level of specialized knowledge for the relevant AML area (e.g., products and services); (c) AML-related certifications and training; and (d) the number of years of AML-related job experience.
### Training and Awareness

Expectations for skilled AML resources continue to rise; there is a growing need for training plans and curricula to be tailored, relevant, frequent, and mandatory. In addition to basic AML training relating to regulatory, legal, and policy requirements, staff should receive training in: (a) all critical AML topics; (b) Business Unit-specific information (e.g., products and services, customers, risk profiles, policies and procedures, etc.); and (c) targeted and more advanced training that is relevant to roles and responsibilities.

### Overall AML Infrastructure, Framework, and Practices (Policies, Procedures and Processes; Management and Oversight; Technology and Operations)

The challenge of managing and overseeing a broad range of AML activities and functions for a large and complex organization requires careful attention to the strength and design of the FI’s AML infrastructure, framework, and related practices.

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

### Management and Oversight

The AML program and associated initiatives should be commensurate with the FI’s risk profile in order to maintain efficient operations, regulatory compliance, and risk management.

### Policies, Procedures, and Processes

Policies and procedures should be documented, approved (e.g., by board of directors, senior management, AML governance committees),
CREATE AN EFFECTIVE AML AUDIT / REVIEW PROGRAM

comprehensive, consistent with best practices and regularly updated to address—and remain current with—critical AML areas (e.g., KYC, suspicious or unusual activity, OFAC and sanctions, training). Exception processes (such as for deviating from global AML policies) should be clearly documented with necessary details (e.g., the approvals that need to be obtained).

OPERATIONS AND TECHNOLOGY
Routine and standard AML operations and functions (e.g., currency transaction reporting, recordkeeping activities, data management, monetary logs, Section 314(b) information sharing, compliance with OFAC and sanctions reporting) should address regulatory requirements and align to the FI’s global AML policy.

Conclusion: A Solid Risk Assessment Method Can Better Equip Audit
Through its role as the eyes and ears of the enterprise, the audit department is uniquely positioned to independently identify AML risks and trends, to inspect the control environment, to test the sustainability of the AML program, to assist the business functions in maintaining effective risk management behaviours, and to intervene as necessary to ensure that potentially material issues are recognized, understood, and addressed. As such, Audit is a vital player and an essential line of defence in protecting the FI and ensuring compliance with regulatory matters and safe business practices.

Although the act of enhancing the design of an Audit risk assessment tool might sound like a small step, the effect can be substantial if it leads to a more accurate, substantive, and reliable audit planning and testing program, one which,
between the regulator’s wealth of aggregate industry knowledge and the auditor’s “inside” operational and technical knowledge, is a much more powerful force for creating an effective AML audit.