ACAMS® | Advancing Financial Crime Professionals Worldwide

White Paper on KYC – Enhanced Due Diligence

Know Your Customer:

Customer Due Diligence (CDD) for a U.S.-Based Financial Institution with a Global Footprint.

In-Depth View on Enhanced Due Diligence, Sanctions, Screening, Risk Scoring and Highlighting Benefits of Global KYC.

CAMS AUDIT

Author: Jagannathan Vasudevan, CAMS

EXECUTIVE SUMMARY

The cornerstone of a strong Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance program includes comprehensive customer due diligence (CDD) policies, procedures and processes for all customers combined with the adoption and implementation of internal controls. The requirement that a financial institution (FI) know its customers, and the risks presented by its customers, is basic and fundamental to the development and implementation of an effective BSA/AML compliance program.

With respect to accounts that have been identified by an institution's CDD procedures as posing a heightened risk, these accounts should be subjected to enhanced due diligence (EDD) that is reasonably designed to enable compliance with the requirements of the BSA. In essence, a FI's CDD processes should commensurate with its BSA/AML risk, with particular focus on high-risk customers.

This paper will focus on enhanced due-diligence (EDD), sanctions, screening, risk scoring and highlighting the benefits of a global approach to CDD (Global KYC) for a U.S.-based FI/Bank operating across geographies with diversified lines of businesses.

Note: Various sources have been referenced for this white paper. Please see the REFERENCES section for further details.

INTRODUCTION

The Currency and Foreign Transactions Reporting Act of 1970 (which legislative framework is commonly referred to as the Bank Secrecy Act" or BSA) requires U.S. FIs to assist U.S. government agencies in detecting and preventing money laundering. An AML program is an essential component of a FI compliance regime.

Adequate due diligence on new and existing customers is a key part of these controls. Without this due diligence, banks are subject to reputational, operational, legal and concentration risks, which can result in significant financial costs.

FIs need to conduct due diligence on its customers by reducing the likelihood of becoming a legal vehicle of financial crime. A sound CDD program is the key to protect the FI's reputation and the overall integrity of the banking systems along with other regulatory requirements.

The Financial Crimes Enforcement Network (FinCEN) is a bureau of the U.S. Department of the Treasury that collects, analyzes and disseminates financial intelligence and engages strategic use of financial authorities. There are four elements (a.k.a pillars) of a BSA/AML compliance program: system of internal controls, designated compliance officer, independent audit and training. FinCEN issued a rule in 2016 that adds a fifth core element as risk-based procedures for conducting ongoing CDD.

Per FinCEN, The key elements of CDD include:

1. Identifying and verifying the identity of customers;
2. Identifying and verifying the identity of beneficial owners of legal entity customers (i.e., the natural persons who own or control legal entities);
3. Understanding the nature and purpose of customer relationships to develop a risk profile;
4. Conducting ongoing monitoring to maintain and update customer information and to identify and report suspicious transactions.

Collectively, these elements comprise the minimum standard of CDD, which FinCEN believes is fundamental to an effective AML program.

As part of the CDD process, it is a common practice to gather the following data elements at a minimum:

- **Geography**: The client's location, place of incorporation, location of wealth and assets, and planned locations for establishing and conducting banking activity;
- **Employment/Business**: Employment information for customers that are individuals and the type, nature and history of the business/organization for customers that are entities;
- **Beneficial Ownership**: Identification information on beneficial owners;
- **Financial Information**: Assets, annual turnover/income, investments and source of wealth;
- **PEP**: Information about whether the client (or beneficial owner, immediate family member or close associate of the client) is, or has ever been affiliated with a government in a significant capacity;
- **Product Profile**: Information on the customer's anticipated banking activity and whether the customer plans to use high-risk products (E.g. Cross-border wire transfer).
- **Reputation**: Reputational information, especially related to criminal charges or convictions.

ENHANCED DUE DILIGENCE (EDD)

International standards proposed by FATF require that a risk-based approach be applied to CDD. Consequently, the measures should be applied on a risk-sensitive basis depending on the type of customer, business relationship or nature of the transactions or activity. Higher-risk customers should be subject to enhanced due diligence.

Clients that pose higher money laundering and terrorist financing risks are subject to enhanced scrutiny, or EDD. This enhanced level of scrutiny provides a more comprehensive understanding of the risks associated with the client, as well as confirmation of factual information provided by the client, to mitigate the risks presented. Some of the scenarios could include but are not limited to senior public figures, private banking, et al.

Risk-based EDD procedures may include:

- Obtaining further information regarding a customer's background;
- Site visit;
- Obtaining more detailed information about a customer's source and structure of wealth;
- Obtaining more detailed information about a customer's source of funds;
- Conducting internet or media searches;

EDD varies based on the type of client. The specific EDD requirements for each client type are highlighted below.

EDD FOR INDIVIDUALS

EDD may be required for individuals who have a high net worth or whose risk rating is HIGH.

EDD may include gathering information including but not limited to:

- Financial statements;
- Source of wealth/funds; and
- Net worth.

Where certain other risk factors are also identified for all individuals, such as senior foreign political figures (SPF) or affiliations to SPF, and/or screening or search matches, also requires additional due diligence.

EDD FOR BUSINESS

EDD is required for higher-risk business/corporations, based on the risk posed, as determined by the results of the CDD process. For example, certain higher risk businesses, such as internet-only businesses, law firms, casinos and cash-intensive businesses that offer ancillary money services, may be subject to EDD.

The required EDD may include but is not limited to:

- Source of funds;
- Information regarding banking relationships maintained with other FIs;
- Names and locations of its customers;
- Names and locations of its suppliers;
- Identifying board members;
- Due diligence on the business entity AML program
- Site visit; and
- Review of the company's website.

Simplified due diligence is allowed for certain publicly-traded corporations because of the due diligence, regulatory oversight and transparency of information requirements of exchanges.

For not-for-profit (NFP) organizations, the collection and review of additional information is required as mentioned below but not limited to:

- Purpose of the organization;
- The entity's organizational structure;
- The organization geographical presence and source of funds;
- How the organization uses funds;
- A list of donors & means by which donations are collected;
- The names and locations of major beneficiaries;
- Aggregate annual grants and contributions, and annual revenue (excluding grants and contributions) for the past two years;
- Due diligence on the NFP's AML program for NFPs that are charities;
- Industry accreditations and affiliations;
- Banking relationships at other financial institutions; and
- Board members.

EDD FOR FINANCIAL INSTITUTIONS

Where certain increased risk factors are identified as part of the CDD process for bank and non-bank FIs (NBFIs), such as the provision of correspondent banking, especially cross-border correspondent banking, or third-party payment processing services, additional EDD information is required to be collected and reviewed.

This is consistent with Section 312 of the USA PATRIOT Act, which requires all U.S. FIs that establish, maintain, administer or manage cross-border correspondent accounts and private banking accounts in the U.S. for non-U.S. persons to establish due diligence, and where necessary, EDD policies, procedures and controls that are reasonably designed to detect and report money laundering through those accounts. While Section 312 applies to U.S. FIs establishing or maintaining accounts for non-U.S. persons in the U.S., the same requirements should be applied to cross-border correspondent and private banking accounts and relationships to all countries and jurisdictions globally. EDD is also required for all high-risk clients.

The required EDD may include but is not limited to:

- Information that identifies correspondent banking risks associated with nested banks (if any);
- Identifying board members and collecting information;
- Payable-through accounts; and
- Financial statements;

EDD FOR GOVERNMENTS

EDD is required for government and embassy clients with increased risk factors or a high-risk jurisdiction. Due diligence procedures may include client site visits and obtaining references or letters of introduction from reliable sources.

Embassies and governments of countries with a low risk rating may require less EDD. Also, the countries that are members of Financial Action Task Force (FATF) or rated high on Transparency International's Corruption Perceptions Index may also be subject to less EDD.

CORRESPONDENT BANKING

Regulators and international AML organizations have identified foreign correspondent banks (FCBs) as potential high-risk clients because these particular relationships provide a direct gateway into local financial systems. Specifically, FCB relationships expose to significant legal, regulatory and reputational risk if the FCB clients have inadequate or

ineffective AML controls, which may increase the ability of the FCB's own clients to launder money through the accounts held at the FI. Appropriate due diligence (EDD when appropriate) is required for all cross-border correspondent accounts.

Here are some of the sections of USA PATRIOT Act on correspondent accounts.

Source: https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act

- **Section 311:** Special Measures for Jurisdictions, Financial Institutions, or International Transactions of Primary Money Laundering Concern

  This section allows for identifying customers using correspondent accounts, including obtaining information comparable to information obtained on domestic customers and prohibiting or imposing conditions on the opening or maintaining in the U.S. of correspondent or payable-through accounts for a foreign banking institution.

- **Section 312**: Special Due Diligence for Correspondent Accounts and Private Banking Accounts

  This section amends the BSA by imposing due diligence & EDD requirements on U.S. FIs that maintain correspondent accounts for foreign FIs or private banking accounts for non-U.S. persons.

- **Section 313**: Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks

  This section is to prevent foreign shell banks from having access to the U.S. financial system. Banks and broker-dealers are prohibited from having correspondent accounts for any foreign bank that does not have a physical presence in any country. Additionally, they are required to take reasonable steps to ensure their correspondent accounts are not used to indirectly provide correspondent services to such banks.

In October 2016, the Office of the Comptroller of the Currency (OCC) issued guidance regarding the periodic evaluation of the risks related to correspondent accounts for foreign FIs (foreign correspondent accounts). The guidance describes corporate governance best practices when evaluating and making account retention or termination decisions. The guidance reiterates OCC's expectation that banks have established policies and procedures for conducting risk assessments for foreign correspondent accounts and periodically evaluates and reassesses the risk as part of their ongoing risk management and due diligence practices.

Correspondent banking services encompass a wide range of services which do not all carry the same level of money laundering/terrorist financing (ML/TF) risks. Some correspondent banking services present a higher ML/TF risk because the correspondent institution processes or executes transactions for its customers' customers.

A correspondent banking relationship can be domestic (both institutions domiciled in the same jurisdiction) or foreign (institutions domiciled in different jurisdictions).

FOREIGN CORRESPONDENT BANKING (FCB) ACCOUNTS

These accounts are:

- Held by a FI for a correspondent bank domiciled in a different jurisdiction; or
- Held by a FI for a correspondent bank domiciled in the same jurisdiction but in a currency different to the national currency of said jurisdiction so long as this account is not set up with the exclusive purpose of participating in an offshore clearing mechanism for the currency of the account.

Due to the high-risk nature,

- In a new client onboarding scenario, if due diligence cannot be performed or completed, it is recommended to immediately cease the onboarding of customer; and
- In an existing client scenario, if the client fails or refuses to provide required information with regards to additional due diligence documentation and alternative sources or solutions have been exhausted, the FI/business must escalate to senior management to evaluate & consider suspending transaction activity in the account or to even terminate the relationship and close the account.

DOMESTIC CORRESPONDENT BANKING (DCB) ACCOUNTS

These accounts are:

- Held by a FI for a correspondent bank domiciled in the same jurisdiction; and
- Held in the national currency of said jurisdiction

Domestic correspondent banks (DCBs) are generally considered to be of lower AML risk than FCBs as they are not in place to allow their customers to gain access to the international financial system.

EDD MEASURES FOR CORRESPONDENT BANKING

There are differences in EDD required for DCBs and FCBs. There may also be applicable local requirements of a country that would need to be considered. In general, the most stringent requirements would be applied.

The EDD measures to be performed shall include, but are not limited to:

- Identification of all natural person(s) who are ultimate beneficial owners of 10 percent or more (5 percent for banks with offshore licenses) of the CB customer;
- Identifying SPFs within the senior management and ownership structure of the correspondent bank and conducting periodic negative media searches and monitoring for transactions;
- Conducting a site visit prior to onboarding;
- Evaluating the correspondent bank clients' AML program to determine to what extent their program is designed to detect and prevent money laundering and evaluate the controls in place surrounding nested activity that may exist within the account;
- Evaluating and documenting correspondent bank clients' sanctions program.
- Documenting an AML risk summary that provides an overall assessment of the financial institution's AML risk profile and its acceptability to the FI.
- Performing periodic transaction reviews
- Determining if the actual activity is in line with the stated purpose of the account;
- Conducting a geographic analysis aimed to identify from where transactions originated or were directed;
- Identifying and analyzing transactions from account-involving shareholders, beneficial owners or senior managers to see if any have been identified as SPFs.

AUDIT PERSPECTIVE:

- Determine if correspondent bank risk framework is tailored to the various categories of higher-risk relationships and determine whether the inherent risk level is justified and if it warrants any further reassessment of risk and risk mitigation plan.
- Determine if correspondent banks/FIs have policies, procedures and processes in place to enable it to identify the ultimate beneficial owners of the account and needs to be convinced that the respondent bank/FI has conducted sufficient due diligence on the customers having direct access to the account of the correspondent institution.
- Review policies and controls in place for freezing action and comply with prohibitions from SDN/entities, per FATF Recommendation #16.
- Ensure processes and controls in place to verify:

- USA PATRIOT Act certifications are obtained within 30 days from the account open date for new relationships.
- Recertifications are obtained every 3 years to maintain existing relationship.
- Process for reviewing information in certification and in case of any misinformation or suspicion, obtains the necessary corrected information within 90 days, failing which
  - FI to take steps to close the account
  - FI may not permit foreign bank to execute any transactions other than the transactions to close the account.

PRIVATE BANKING

Private banking (PB) provides highly personalized and confidential products and services to high net worth clients at fees that are often based on “assets under management.”

PB caters to wealthy customers who seek confidentiality and personalized service. PB is an extremely lucrative, competitive and worldwide industry.

A "private banking account" is an account (or any combination of accounts) maintained at a bank that satisfies all three of the following criteria:

- Requires a minimum aggregate deposit of funds or other assets of no less than $1,000,000.
- Is established on behalf of or for the benefit of one or more non-U.S. persons who are direct or beneficial owners of the account.
- Is assigned to, or is administered by, in whole or in part, an officer, employee or agent of a bank acting as a liaison between a FI covered by the regulation and the direct or beneficial owner of the account.

The following factors may contribute to the vulnerabilities of private banking with regard to money laundering:

- Perceived high profitability
- Intense competition
- Powerful clientele
- The high level of confidentiality associated with private banking

Risks and methods of money laundering and terrorist financing:

- The close relationship of trust developed between relationship managers and their clients.

- Commission-based compensation for relationship managers.
- A culture of secrecy and discretion developed by the relationship managers for their clients.
- The relationship managers becoming client advocates to protect their clients.

EDD MEASURES FOR PRIVATE BANKING

- Additional ownership information: Ascertain the identity of all nominal and beneficial owners of a private banking account.
- Ascertain whether the nominal or beneficial owner of any private banking account is a SPF. Note: SPF is covered in detail on the next section (POLITICALLY EXPOSED PERSON)
- Verification of funds and funding sources: Ascertain the source(s) of funds deposited into a private banking account and the purpose and expected use of the account.
- Review the activity of the account to ensure that it is consistent with the information obtained about the client's source of funds, and with the stated purpose and expected use of the account, and to file a SAR, as appropriate, to report any known or suspected money laundering or suspicious activity conducted to, from, or through a private banking account.
- Negative news screening;
- Periodic review: Procedures describing the periodic review process at a minimum include the following customer types to be reviewed and screened on an annual basis:
    - SPFs
    - Bearer share entities
    - Money service businesses
    - Embassies
    - Designated high-risk clients

The below relationships and accounts must be prohibited:

- Shell banks;
- Sanctioned individuals, entities, countries and/or governments

- Individuals, entities or countries designated by the U.S. Department of the Treasury as a Primary Money Laundering Concern or Money Laundering Concern pursuant to the USA PATRIOT Act, Section 311;
- Individuals or entities convicted of money laundering and/or terrorist financing;
- Wholly anonymous beneficial owners;
- Operating accounts for casinos/internet gambling businesses

Enhanced scrutiny of private banking accounts for PEP/SPF is covered in the next section- POLITICALLY EXPOSED PERSON [PEP].

AUDIT PERSPECTIVE:

Determine if the FI has implemented policies, procedures and controls for private banking accounts established, maintained, administered or managed in the U.S. for non-U.S. persons and the due diligence program includes reasonable steps to:

- Ascertain the identity of the nominal and beneficial owners of a private banking account (31 CFR 103.178(b)(1)).
- Ascertain whether any nominal or beneficial owner of a private banking account is a senior foreign political figure (31 CFR 103.178(b)(2)).
- Ascertain the source(s) of funds deposited into a private banking account and the purpose and expected use of the private banking account for non-U.S. persons (31 CFR 103.178(b)(3)).
- Review the activity of the account to ensure that it is consistent with the information obtained about the client's source of funds and with the stated purpose and expected use of the account, as needed, to guard against money laundering and to report any known or suspected money laundering or suspicious activity conducted to, from, or through a private banking account for non-U.S. persons (31 CFR 103.178(b)(4)).

POLITICALLY EXPOSED PERSON [PEP]

The term PEP generally includes a current or former senior foreign political figure, their immediate family and their close associates.

Per FFIEC Exam Manual, a SPF is a

- Senior official in the executive, legislative, administrative, military or judicial branch of a foreign government (whether elected or not), a senior official of a major foreign political party or a senior executive of a foreign government-owned corporation. In

addition, a SPF includes any corporation, business or other entity that has been formed by, or for the benefit of, a SPF.

- The immediate family of a SPF typically includes the figure's parents, siblings, spouse, children and in-laws.
- A close associate of a SPF is a person who is widely and publicly known to maintain an unusually close relationship with the SPF, and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of the SPF.

While the terms SPF and PEP are often used interchangeably, PEP is a broader category that may also include persons who may not be considered SPFs. The determination that a particular person qualifies as an SPF is based on the person's responsibilities within the government, level of authority and influence over government activities, and/or access to government assets and funds. As a rule, an SPF does not encompass middle-ranking or more junior individuals.

SPF encompasses both foreign and domestic PEPs.

Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, for example, heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials, etc.

Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials, etc.

Per FATF recommendation, FIs should be required, in relation to foreign PEPs (whether as a customer or beneficial owner), in addition to performing normal CDD measures, to:

a) Have appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;
b) Obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
c) Take reasonable measures to establish the source of wealth and source of funds; and
d) Conduct enhanced ongoing monitoring of the business relationship.

Certain types of SPFs may present a higher level of risk due to the prominence of their positions (prominent SPFs). Who are subject to EDD and monitoring?

Prominent SPFs include:

- Heads and deputies - state/national government;
- National government ministers;
- Members of the National Legislature;
- Heads of the Armed Forces; and
- Senior members of the Judiciary.

Close associates and immediate family members of prominent SPFs are subject to the EDD applicable to prominent SPFs.

As part of risk-based due diligence, the data below may be gathered but is not limited to:

- Title and details on the position the SPF holds or held, including the level of influence or prominence of the position or his/her status as an immediate family member or close associate;
- The SPF's reputation and family background;
- The SPF's current access to or ability to move government funds, as well as his/her control/influence over strategic national assets (e.g., natural resources, ports or airport hubs, refineries, offshore platforms, military bases);
- The SPF's source of wealth, including whether he/she derives revenue from government sources. Additionally, the business must take reasonable steps to independently corroborate source of wealth, wherever available. See the Source of Wealth Standard;
- Adverse media searches through a Citi-approved vendor to identify and assess publicly-available negative information; and

Assessment of overall SPF risk associated with this client and whether there are significant risks or issues identified in the due diligence process.

ENHANCED DUE DILIGENCE FOR SPF

In addition to due diligence mentioned above, It is also highly recommended to get risk acceptance approval/clearance from FI senior management and the head of compliance for the country in which the SPF holds the position. The approval has to be secured before establishing the client relationship. SPF accounts are also subject to enhanced monitoring which includes transaction monitoring and periodic review of accounts, to ensure the activity is in line with purpose of account, anticipated usage and source of funds.

When the due diligence cannot be performed, subject to local law, the FI needs to do one of the following: A. Refuse to open the account; B. Close the account; C. Suspend the transaction(s) or D. Escalate to senior management / country level head.

AUDIT PERSPECTIVE:

- In case the PEP determination is made after the account is opened
  - What controls are in place to evaluate the risks?
  - What process and documentation are in place for the approval process?
- Review the overall process of identifying PEPs both manually and systematically (domestic & foreign PEPs).

INTERSECTION OF SCREENING AND KYC

The FATF is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF recommendations are recognized as the global AML and counter-terrorist financing (CTF) standard.

Recommendation 6 requires each country to implement the targeted financial sanctions regimes to comply with the United Nations Security Council resolutions (UNSCRs or resolutions) relating to the prevention and suppression of terrorism and terrorist financing. Efforts to combat terrorist financing are greatly undermined if countries do not freeze the funds or other assets of designated persons and entities quickly and effectively.

Effective freezing regimes are critical to combating the financing of terrorism and, as a preventive tool, accomplish much more than freezing terrorist-related funds or other assets present at any particular time.

As part of its enforcement efforts, the Office of Foreign Assets Control (OFAC) publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups and entities, such as terrorists and narcotics traffickers, designated under programs that are not country-specific. Collectively, such individuals and companies are called Specially Designated Nationals or SDNs. Their assets are blocked and U.S. persons are generally prohibited from dealing with them. The SDN list maintained by OFAC is a living and breathing document. It is not a “free standing” document. The prohibitions against dealing with any particular SDN correspond to the executive order, law or regulations under which the individual or entity has been designated.

A FI must establish and maintain processes and controls that are consistent with applicable laws and regulatory requirements and obligations under U.S. and non-U.S. sanctions regulations. The consequences for violating sanctions can be severe. In the U.S., for example, violations can be punished with large monetary penalties and, in serious cases, criminal penalties.

U.S SANCTIONS

OFAC administers and enforces economic and trade sanctions against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction and other threats to the national security, foreign policy or economy of the U.S., based on U.S. foreign policy and national security goals.

U.S. sanctions prohibit certain financial and other transactions and require blocking of assets under U.S. jurisdiction. FIs must avoid providing services (e.g., opening or maintaining accounts, financing, funds transfers) to individuals and entities identified by OFAC as associated with narcotics trafficking, terrorism or the proliferation of weapons of mass destruction. FIs must file reports of rejected transactions and blocked property with OFAC. The prohibitions set forth in U.S. sanctions apply to U.S. persons, which are defined as:

- Individuals who are citizens or permanent resident aliens (“green card holders”) of the U.S., wherever located;
- Entities organized under the laws of, or located in the U.S. or any jurisdiction within the U.S., including their foreign branches; and
- Individuals located in the U.S., even if temporarily.

NON–U.S. SANCTIONS

Non-U.S. sanctions are typically based on U.N. and/or multilateral mandates (e.g., European Union (EU) sanctions) that are administered and enforced by local governmental authorities (e.g., the U.K.’s Her Majesty’s Treasury). The range of sanctions may include comprehensive economic and trade sanctions and/or more targeted measures such as arms embargos, travel bans or financial or diplomatic restrictions. Non-U.S. sanctions may require the blocking or freezing of assets or financial transactions of sanctions targets.

SCREENING

FIs are responsible for screening individual and entities with whom doing business is prohibited. Screening is required for account holders, beneficial owners and other affiliates related to customer account(s). Screening has to be performed both at the time of onboarding and ongoing (periodically – timeline would vary based on the risk of customer).

There are two categories of screening activities namely

- Sanctions Screening: Screening conducted against OFAC sanctions listings and jurisdictions subject to sanctions imposed by the U.S. (U.S sanctions) and against any non-U.S sanctions listing issued and jurisdictions subject to sanctions pursuant to local sanctions law and regulations applicable to their transactions. The below will categories will have to be screened:
    - Accounts: Any type of accounts (E.g., deposit, credit, et al.)
    - Relationships: Individual/entity in a formal relationship to receive services
    - Transactions: Any type of financial transaction (E.g., Wire transfer)
- AML Name Screening: This comprises of three specific types namely:
    - SPF Screening: To identify customers deemed to be SPFs.
    - Watch List Screening: To discern a client reputation and/or involvement in any criminal activity by screening against criminal enterprise and other non-sanctions law enforcement lists and databases.
    - Adverse Media: Primarily to find if the client is involved in any criminal activities and/or adverse reputation by screening against well-known, reputable information sources. Example: FACTIVA is a product providing such service.

A sanctions match occurs when, as part of the screening process, a name, or other relevant information on an account, relationship, securities holding or transaction is sufficiently similar to a name on a sanctions list (E.g., OFAC's SDN list). Hits must be reviewed and disposition appropriately and even escalated to senior management in certain situations.

In the course of developing or maintaining a sanctions screening program, FIs sometimes develop a "false hit list" comprised of individuals and entities whose characteristics trigger a screening match to one or more entries on the SDN list or other sanctions criteria, but who, after a thorough review, are determined not to be SDNs, blocked persons or affiliated with a country, region or activity subject to OFAC-administered sanctions. In the case of software screening tools, once an individual or entity is added to the false hit list, the screening software typically will suppress an alert (or will otherwise bypass an alert)

associated with the individual or entity, thereby eliminating any transaction hold, or prompting further manual review of, such parties in the absence of other alerts.

While false hit lists represent a common and legitimate practice, and are generally designed to reduce the volume of OFAC-related matches that a U.S. person has determined are false, it is important to implement policies and procedures designed to review, evaluate and reassess the parties that are included on such lists.

Given the dynamic and changing environment of U.S. economic sanctions programs, these measures could include:

- Involving sanctions compliance personnel in developing guidelines for, and oversight of, the functioning of false hit lists, including periodic reviews;
- In situations where additions or changes to an SDN list entry are similar to a false hit list entry, ensuring that alerts generated by screening hits in connection with the additions/changes to the SDN list are not automatically suppressed by the existing false hit list entry;
- Amending the false hit list, as needed, in response to updates to OFAC's sanctions programs (including, for example, the revocation of general licenses, the implementation of new sanctions programs and/or prohibitions, or enhanced restrictions on certain categories of transactions); For direct customers who have an entry on a false hit list, ensuring that any meaningful changes to the customer's information (E.g., a change in ownership status, business activity, address, date of birth, place of business, etc.) trigger a review of the false hit list entry.

AUDIT PERSPECTIVE:

- Sanctions policy document must be maintained, periodically updated and controlled. It is recommended that any changes to policy document need to be reported to senior management in the compliance department who may in turn bring it to the attention of the board of directors, if need be.
- Review the periodic test plan and test results of sanctions program implementation.
- Training: Ensure staff are periodically adequately trained on sanctions and screening.
- Check the screening test results to ensure controls in place as FI's prohibit providing services to individuals and entities identified in SDN/SDNT/SDNTK, et al.
- Review false positive matches to determine if they are being reviewed within a reasonable timeframe and with sufficient dispositioning rationale.

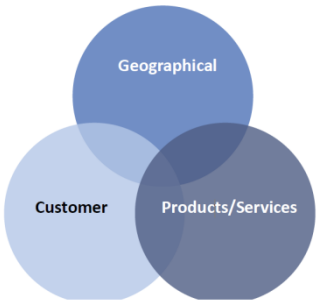
- Ensure filter criteria and sanctions list are up-to-date with the most recent OFAC list.
- Review the reporting procedures to appropriate authorities. E.g., reports to OFAC on blocked transactions/properties.
- Review the policy document on conflict of law: Some countries have regulations that prohibit compliance with certain requirements of U.S. sanctions. For example, if screening a customer results in a positive match that may be impacted by a conflict of law, what are the policies and procedures in place.

CUSTOMER RISK RATING / RISK SCORING

The risk-based approach (RBA) recognizes that not all aspects of an institution's business present the same level of risk. Certain aspects of the institution may pose greater money laundering risks than others and will require additional controls to mitigate these risks, while others will present a minimal risk and will not need the same level of attention. All of the CDD/EDD information captured (topics discussed in prior sections) will become input to determine the risk of customer.

RBA requires institutions to have systems and controls that commensurate with the specific risks of money laundering and terrorist financing facing them. A RBA is preferable to a more prescriptive approach as it is flexible, effective and proportionate.

Risk Factors:



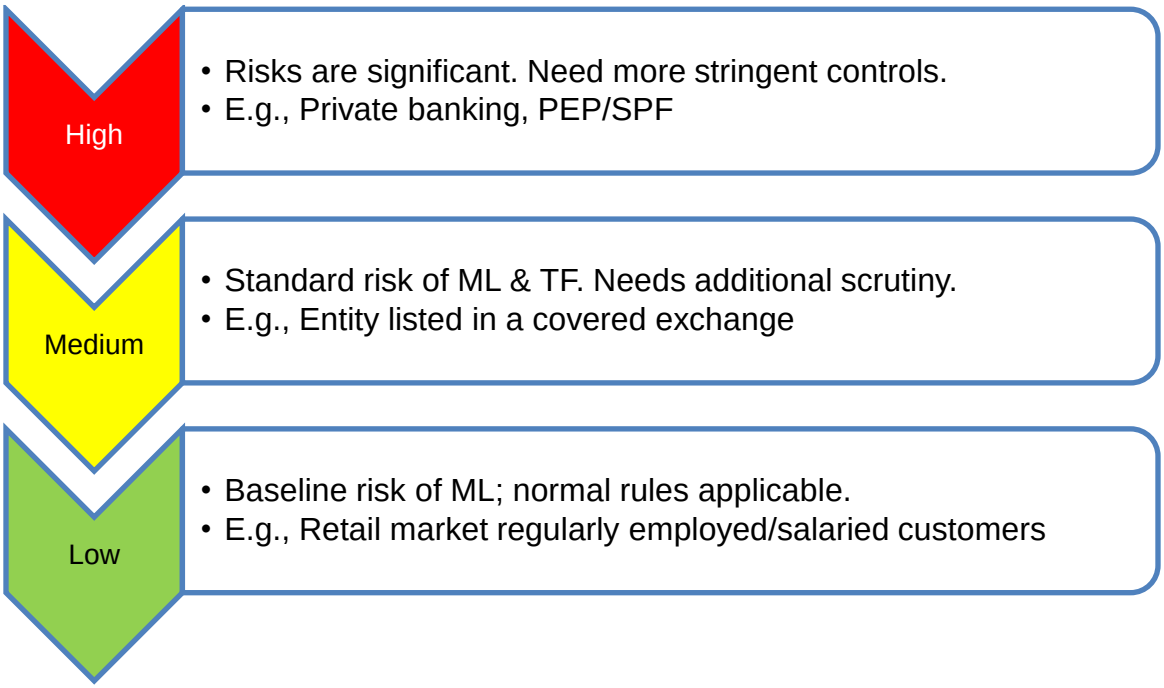
- **Client Type**: Type of client. E.g., individual, PEP, import and export companies.
- **Geography**: Jurisdiction of the client and business counterparties. E.g., sanctions countries.
- **Product/Service**: The various products and services which could expose greater risk. E.g., private banking, cross-border wire transfer.

In addition to above mentioned factors, there are also other factors that determine risk namely type of business, length of relationship, relationship history (e.g. prior subject of SAR filing) et al.

Risk Modeling/Risk Scoring:

Risk score is a numerical representation of the risk of client which is based on the risk model. If the customer risk scoring model is automated (using software), it increases the operational efficiency and reduces human subjectivity in customer risk scoring. The main purpose is to help accurately identify high-risk customers. Each risk factor is given a weightage. The assessment of risk factors may be FI specific, and a conclusion regarding the risk profile should be based on a consideration of all pertinent information. An FI may determine that some factors should be weighed more heavily than others.

The score is a reflection of the potential risks that customer poses. Based on the risk score, clients can be bucketed into different risk level or risk class. They can be categorized as simple as high, medium, low or they could be more elaborate as very high, high, medium-high, medium, low, et al. It is up to the FI to categorize the risks and define standards, processes and controls to monitor and mitigate risks.



The disk scoring model should be able to access customer risk holistically (across all lines of business). As an example, if a customer maintains accounts across multiple lines of business, the risk model should, as much is feasible, assess that customer's risk by factoring all accounts. If that assessment cannot be addressed holistically in a systematic way, the FI should document the limitation and consider developing a process outside of the scoring model to aggregate the overall risk of the customer.

The AML risk assessment in various areas of exposure enables a FI/bank to define the customer acceptance criteria which will become the basis of CDD/KYC program. It is extremely important to determine and periodically reassess the risk rating of a customer which is a key factor in determining the need to perform certain EDD procedures, thefrequency of period review of customer, thresholds for monitoring, et al.

AUDIT PERSPECTIVE:

- Ensure the client risk scoring model and rules are periodically evaluated so that it is aligned to the overall institution's risk profile.
    - The risk scoring model should attribute the scoring to each element of risk in a way that accurately reflects the element's inherited risk
- If risk scores can be manually adjusted or overridden
    - What are those scenarios?
    - Have they been documented?
    - What are the controls in place for approval?

GLOBAL APPROACH TO KYC

Global FIs offer a wide array of services in the area of investment banking, retail banking, commercial banking, mortgage, trading, credit card, brokerage services and much more across the globe. Many large FI have an expanded geographical presence in over 100+ countries. FIs that operate outside of their home jurisdictions have the additional requirement of complying with all the regulations imposed in each jurisdiction in which they operate.

Here are few of the regulatory authorities and regulations (Not a complete list):

Country	Regulatory Bodies	Regulations
United States	SEC, FINCEN, FINRA, OCC, NAIC, NCUA, CFTC	• Bank Secrecy Act (1970), • Money Laundering Control Act (1986), • Money Laundering Suppression Act (1994), • USA PATRIOT Act (2001)
United Kingdom	FCA, PANEL, FPC	• The Money Laundering, Terrorist Financing and Transfer of Funds Regulations (2017)

		• The Proceeds of Crime Act(2002), Serious Crime Act (2005) • The Money Laundering Regulations (2007) • The Terrorism Act (2000)

KYC policies are made mandatory to any FI across the world by regulatory bodies. Particularly, the U.S has more stringent activity and vigilance from regulators in dealing with AML/CTF. Violations of AML laws and regulations carry both civil and criminal penalties. There have been several enforcement actions on FIs for AML non-compliance resulting in heavy fines. One such instance was a France-based FI fined about $8.9 billion for violating sanctions on Sundan, Iran and Cuba.

In a large FI, it is not uncommon to see numerous customer on boarding/KYC systems. Some FI's have KYC systems that are specific to a country, line of business, et al. This leads to different operating procedures by multiple teams. Just as an example, even to collect and store the KYC documentation, there could be inconsistency in procedures. Multiple KYC systems also do not provide a single view of the customer. An organization has to look at multiple systems to get a consolidated view which could be manually intensive and not always accurate. This is a serious issue when it comes to managing enterprise-level AML risk.

A global approach to KYC can yield the following benefits

- **Platform consolidation**: Opportunity to consolidate multiple onboarding/KYC platforms which could save money over a period of time. There will be an upfront cost/investment in building a consolidated platform though.
- **Consistent standards, policies and procedures**: Enforcing standards across all lines of business and geographies will lead to consistency and operational efficiencies.
- **Faster turn-around time:** Regulations are always evolving. Having a centralized platform will help meet the regulatory requirements much faster compared to a fragmented approach where multiple KYC/onboarding systems need to be changed.
- **Enterprise-wide risk management**: A single view of centralized repository equips the FI to generate MIS reporting capabilities which helps to determine the exposure level and mitigate risk across the organization. This can also help make a decision on terminating the relationship with certain high-risk customers/geographies/products/services.

CONCLUSION

No FI can reasonably be expected to detect all wrongdoing by customers, including money laundering. But if an institution develops systems and procedures to detect, monitor and report the riskier customers and transactions, it will increase its chances of staying out of harm's way from criminals and from government sanctions and penalties.

AML regulations are not static. Policies, procedures and internal controls need to evolve based on regulatory changes and expectations. A well-developed enterprise-wide risk assessment will assist in identifying the FI's BSA/AML risk profile. Understanding the risk profile enables the FI to institutionalize appropriate risk management processes and mitigate risks.

By a robust CDD, FIs know their customers, who they are and what transactions they conduct which are critical aspects in combating all forms of illicit financial activity, from terrorist financing and sanctions evasion to more traditional financial crimes, including money laundering, fraud and tax evasion.

Sound KYC procedures are critical in managing a bank or non-bank FI. The basel committee recommendation is also to have KYC practices be part of risk management and internal control systems.

APPENDIX

ACRONYMS

AML	ANTI MONEY LAUNDERING
CTF	COUNTER TERRORIST FINANCING
BCBS	BASEL COMMITTEE ON BANKING SUPERVISION
CDD	CUSTOMER DUE DILIGENCE
EDD	ENHANCED DUE DILIGENCE
SDD	SIMPLIFIED DUE DILIGENCE
FI	FINANCIAL INSTITUTION
SAR	SUSPICIOUS ACTIVITY REPORT
DNFBP	DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSION
NFP	NOT FOR PROFIT ORGANIZATION

RBA	RISK BASED APPROACH
FATF	FINANCIAL ACTION TASK FORCE
FINCEN	FINANCIAL CRIMES ENFORCEMENT NETWORK
FINRA	FINANCIAL INDUSTRY REGULATORY AUTHORITY
SDN	SPECIALLY DESIGNATED NATIONAL
SDNTK	SPECIALLY DESIGNATED NARCOTICS TRAFFICKING KINGPIN
OFAC	OFFICE OF FOREIGN ASSETS CONTROL
OCC	OFFFICE OF COMPTROLLER OF ACCOUNTS
BSA	BANK SECRECY ACT
PEP	POLITICALLY EXPOSED PERSON
SPF	SENIOR POLITICAL FIGURE
LOB	LINE OF BUSINESS
NBFI	NON BANKING FINANCIAL INSTITUTION
FCA	FINANCIAL CONDUCT AUTHORITY (U.K)
FPC	FINANCIAL POLICY COMMITTEE (U.K)
UNSCR	UNITED NATIONS SECURITY COUNCIL RESOLUTIONS
FCB	FOREIGN CORRESPONDENT BANK

REFERENCES

- https://www.federalregister.gov/documents/2016/05/11/2016-10567/customer-due-diligence-requirements-for-financial-institutions
- http://files.acams.org/pdfs/2016/Benefits_of_an_Effective_CDD_Program_and_How_Risk_D_Bruggeman.pdf
- https://www.financialservicesperspectives.com/2016/07/the-fifth-pillar-of-amlbsa-compliance-fincen-issues-final-rule-for-new-customer-due-diligence-requirements-under-the-bank-secrecy-act/
- http://www.klgates.com/fincen-adopts-new-customer-due-diligence-requirements-for-financial-institutions-07-26-2016/
- https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2013-a003
- https://www.fincen.gov/sites/default/files/2016-09/FAQs_for_CDD_Final_Rule_%287_15_16%29.pdf
- https://www.trulioo.com/blog/ensure-cip-runs-smooth/

- https://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Documents/staterule.pdf
- https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_011.htm
- https://www.un.org/sc/ctc/wp-content/uploads/2016/03/fatf-rec05.pdf
- http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf
- https://www.int-comp.org/careers/a-career-in-aml/what-is-cdd/
- https://www.lexology.com/library/detail.aspx?g=f392fd40-0f77-4fff-ab3e-e7b0fc46f982
- https://www.sec.gov/about/offices/ocie/amlsourcetool.htm
- https://www.sec.gov/about/offices/ocie/amlsourcetool.htm#4
- https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=aab3521f5c9a9c5fd799519e54a3d34a&mc=true&n=pt31.3.1023&r=PART&ty=HTML#se31.3.1023_1220
- https://www.fincen.gov/sites/default/files/shared/31_CFR_Part_103_312_EDD_Rule.pdf
- https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_047.htm
- https://www.occ.gov/news-issuances/bulletins/2016/bulletin-2016-32.html
- https://www.occ.gov/topics/compliance-bsa/foreign-correspondent-banking-fact-sheet.pdf
- http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf
- http://www.fatf-gafi.org/publications/fatfrecommendations/documents/correspondent-banking-services.html
- http://m.bankingexchange.com/news-feed/item/6739-breaking-down-beneficial-ownership
- https://www.crowehorwath.com/folio-pdf/The-Changing-Face-of-Customer-Risk-Scoring-Compliance_FS-16000-004G.pdf
- https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx
- https://www.law360.com/articles/262952/4-steps-toward-ofac-sanctions-compliance
- http://www.acams.org/wp-content/uploads/2015/08/The-Auditors-Expectations-Knowing-the-Customers-and-Proving-It-Mark-Wolfrey.pdf

- https://www.fincen.gov/sites/default/files/shared/CDD-NPRM-Final.pdf
- Various Banking & Consulting firm websites (PWC, Protiviti, et al)
- ACAMS training Materials and