# How to Audit Know Your Customer (KYC) and Customer Due Diligence (CDD)

Sohail Akbar

The intended purpose of this white paper is to define the importance of the KYC and CDD program and audit's role in assessing the adequacy to help ensure that the program is robust in order to meet the regulatory requirements and expectations.

**October 2018**

# Contents

## *Executive Summary*

In recent years, significant focus has been on the monitoring of transactions and sanctions screening requirements, but not as much on the Know Your Customer (KYC) and Customer Due Diligence (CDD) requirements.

Several methodologies are used by money launderers to move illegitimate money into legitimate institutions. An example of one method often practiced by money launderers is the movement of money into a financial system through the use of multiple cash deposits, checks, credit cards, investment products, and insurance and wire transfers.

Such practices place financial institutions (FIs) (banks, money service businesses, credit unions, stock brokerage firms, insurance companies, finance companies, etc.) at risk of unknowingly becoming complicit in a money laundering action if the financial institutions lack a sufficient system of internal controls to identify and mitigate such risk exposure.

To manage this risk, FIs have incorporated, among other internal controls, customer CDD requirements based on the KYC principle as part of their anti-money laundering (AML) strategies. These KYC and CDD policies require that financial institutions identify and verify the identity of customers on the basis of the information either through documentary means (e.g., unexpired government issued identification) or non-documentary means (e.g., checking references with other financial institutions).

The responsibility for identifying customers has been complicated by the difficulties inherent in identifying beneficial owners (i.e., "the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted"). A strong KYC and CDD provide a solid baseline for the financial institutions to uncover the true ownership and protect the financial systems from falling victim to perpetrators.

A robust KYC/CDD program is the basis of identifying potential money laundering and also serves as the basis of identifying sanctions exposure. However, organizations have been focusing on developing transaction monitoring and sanctions screening software/tools and have not developed robust controls in the areas of KYC/CDD.

In order to have effective AML monitoring and sanctions screening processes, it is vital for an organization to have updated customer information and to perform the required due diligence on customer profiles.

The purpose of this white paper is to explain the importance of KYC/CDD and the role of auditors in ensuring that required testing is performed, and that the issues uncovered during audit are remediated prior to the regulator's examination or the financial institution (FI) falling victim to the perpetrators of money laundering and terrorism financing.

## *Introduction*

The primary objective of this white paper is to assess the appropriateness and comprehensiveness of financial institutions' (FIs) Know Your Customer (KYC) and Customer Due Diligence (CDD) policies, procedures, and processes for obtaining customer information and assess the value of this information in detecting, monitoring, and reporting potentially suspicious or unusual activity.

The Federal Financial Institutions Examination Council (FFIEC) states that independent testing should be conducted by an internal audit department, outside auditors, consultants, or other qualified independent parties. While the frequency of audit is not specifically defined in any statute, a sound practice is for an FI to conduct independent testing generally every 12 to 18 months, commensurate with its policies, procedures, and anti-money laundering risk profile. The persons conducting the AML testing should report directly to the board of directors or to a designated board committee composed primarily or completely of outside directors. FIs that employ outside auditors or consultants should ensure that qualified persons doing the required testing are not involved in another function of an FI, such as training or developing policies and procedures that may present a conflict or lack of independence.

## 1. Role of Internal Audit

In the context of tightening financial crime regulatory requirements in a constantly evolving risk landscape, internal audit has a crucial role to play in financial institutions to mitigate financial crime risk sustainably; however, internal audit also has a role in the development of appropriate risk assessment tools to constantly monitor and validate their reliability and usefulness.

Independent audit testing of customer due diligence should, at a minimum, include:

- Reviewing the adequacy and comprehensiveness of KYC/CDD policies and procedures to determine whether they are aligned to internal processes and cover the applicable regulatory requirements.
- Performing walkthroughs to understand the knowledge and experience of staff responsible for onboarding customers.
- Reviewing the customer-risk rating methodology and processes.
- Reviewing a sample of new accounts opening from operating effectiveness.
- Reviewing and testing of high-risk accounts and periodic high-risk review processes.
- An evaluation of the overall adequacy and effectiveness of the Customer Due Diligence program, including policies, procedures, and processes.
- A review of FI risk assessment for reasonableness given FI risk profile (products, services, customers, entities, and geographic locations).
- Appropriate risk-based transaction testing with respect to the customer profile to verify an FI adherence to its policies and procedures, record keeping, and reporting requirements.
- An evaluation of management's efforts to resolve violations and deficiencies noted in previous audits and regulatory examinations.
- A review of staff training for adequacy, accuracy, and completeness.
- An assessment of the integrity and accuracy of the Management Information System (MIS) used.

## 2. Importance of KYC/CDD

There was a time when a wire transfer might have come in with the "By Order" party listed as "My Good Customer," terms which no longer exist. That statement sums up AML/KYC risk.

Essentially, there is no such thing as "My Good Customer." All customers, irrespective of origin, charter, or impeccability, carry some degree of risk. The challenge to the financial institution comes in the form of identifying the customer and the potential level of risk occupied by the customer's surroundings. It is insufficient to see a customer, whether an individual or legal entity, as someone or something unto itself. Overlooking a customer's relationships may result in serious difficulties for financial institutions (FIs) as the customer's relationship with the institution develops.

It is evident that some products and services carry higher risks than others, such as USD Dollar Clearing and Trade Finance compared with certificates of deposits (CDs) and individual retirement accounts (IRAs). In addition, some parts of the world pose higher money laundering and/or terrorist financing risks than others, such as North Korea and Iran, compared with the United States and Canada. But no matter which products,

services, and countries carry a higher risk, no product, service, or country has ever conducted a money laundering or terrorist financing activity, but individuals do. There is always someone, whether as individuals, companies, governments, or charities, behind the activity.

That makes the management of KYC risk a critical component of a robust AML compliance program.

A sound KYC/CDD program includes strong customer acceptance, identification, and account-opening procedures, which allow the institution to determine the true identity of each customer and to assess the risk or potential risk presented by the customer.

The foremost tool of Anti-Money Laundering/Combating Terrorist Financing policies (AML/CFT) and procedures is to know your customers before entering into business with them. This involves efforts to determine whether a customer relationship complies with an FI's acceptance criteria, the true identity and beneficial ownership of accounts, the source of funds, the source of wealth, and the nature of a customer's business.

Financial institutions' KYC process traditionally consists of elements that include:

- Customer Identification Process (CIP)
- Customer Due Diligence Process (CDD)
- Enhance Due Diligence Process (EDD)

Similarly, the CDD process includes:

- Customer Identification Program (CIP)
- Initial due diligence
- Ongoing monitoring and enhanced due diligence
- Reporting and escalation

In addition to the four basic elements listed above, a sound CDD program should include these seven additional elements, at a minimum:

- Full identification of customer and business entities, including the source of funds and wealth when appropriate.
- Development of transactional activity profiles of each customer's anticipated activity.
- Definition and acceptance of the customer in the context of specific products and services.
- Assessment and grading of risks that the customer or the account presents.
- Account and transaction monitoring based on the risks presented.
- Investigation and examination of unusual customer or account activity.
- Documentation of findings.

At the time when financial institutions were found to have inadequate AML programs, specifically lacking in KYC or a formal CDD program, they were subjected to large fines and their reputations suffered greatly through public exposure. Below is an extract from an enforcement action that focused on KYC issues, among others:

*"Deutsche Bank has uncovered shortcomings in its ability to fully identify clients and the source of their wealth. In two confidential reviews, dated June 5th and July 9th, Germany's biggest lender detailed the results of tests on a sample of investment bank customer files in several countries, including the Republic of Ireland and Russia.*
*"Both reviews found gaps in the Deutsche Bank screening process, which aims to meet the so-called 'know your customer' (KYC) requirements that are a cornerstone of global anti-money laundering controls. Recent reports issued by regulators show that the bank is still grappling to ensure it knows who it is dealing with…."*

However, because of the costs and time required for AML compliance, financial institutions that understand the importance of implementing a strong AML program will quickly realize KYC/CDD's worth. In today's world, any financial institution that does not appreciate the importance of a strong AML program targeting KYC and CDD programs must also understand the ramification of non-compliance, such as potential monetary penalties and reputational risk. When there is a strong KYC program, the risk of financial loss due to penalties can be mitigated along with various other regulatory, concentration, legal, and reputational risks.

## 3. KYC/CDD Impact on Transaction Monitoring and Sanctions Screening

CDD processes should include periodic risk-based monitoring of the customer relationship to determine whether there are substantive changes to the original CDD information (e.g., change in employment or business operations).

The process of KYC/CDD, sanctions screening, and transactions monitoring are interrelated. The better the KYC/CDD process applied by a financial institution, the more effective the transaction monitoring result it will yield for FIs.

For effective KYC/CDD implementation, sanctions screening plays an important role. It helps an FI identify the true identity of its customer, whether an individual or an entity prior to client onboarding, and it helps FI decide whether the customer is a prohibited, high, medium, or low risk.

Beyond matching names, a key aspect of KYC/CDD controls is to monitor the transactions of a customer against a recorded profile, history of the customer's transactions, and check if the purpose of the transactions is commensurate with the actual activity of the customer.

Transaction monitoring forms part of an organization's governance, risk, and compliance program and when combined with anti-money laundering (AML) and Know Your Customer (KYC) processes, transaction monitoring becomes a highly effective mechanism for revealing the risk that may be hiding between client and institution relationships. KYC/CDD uncovers the customer's level of risk, and it is at this time when FIs monitor customer behavior on a risk-based approach.

The concept of CDD begins with verifying the customer's identity and assessing the risk associated with that customer. Processes should also include enhanced CDD for higher-risk customers and ongoing due diligence of the customer base.

The cornerstone of a strong AML compliance program is the adoption and implementation of comprehensive KYC/CDD policies, procedures, and processes for all customers, particularly those that present a higher risk of money laundering and terrorist financing. The objective of CDD should be to enable FIs to predict with relative certainty the types of transactions in which a customer is likely to engage. These processes assist banks and other financial institutions in determining potentially suspicious transactions when a customer transaction pattern deviates from the information that he or she initially provided at the time of onboarding.

Effective CDD policies, procedures, and processes provide the critical framework that enables FIs to comply with regulatory requirements and to report suspicious activities.

CDD policies, procedures, and processes are crucial to FIs because they aid in:

- Detecting and reporting unusual or suspicious transactions that potentially expose an FI to financial loss, increased expenses with remediation efforts, or reputational risk.
- Assist in detecting and potentially mitigating criminal exposure from persons who use or attempt to use an FI's products and services for illicit purposes.
- Making sure the FI adheres to safe and sound banking practices.

Management should have a thorough understanding of money laundering or terrorist financing risks of an FI's customer base. Under this approach, banks and other FIs should obtain information at account opening sufficient to develop an understanding of normal and expected activity for the customer's occupation or business operations. This understanding may be based on account type or customer classification.

This information should allow FIs to determine the customer's risk profile at account opening. Banks, MSBs, securities and insurance firms, etc., should monitor their lower-risk customers through regular suspicious-activity monitoring and customer due diligence processes. If there is an indication of a potential change in the customer's risk profile (e.g., expected account activity, change in employment or business operations), management should reassess the customer risk rating and follow established policies and procedures for maintaining or changing customer risk ratings.
Institutions should have processes or a timeline for reviewing all customers (high, medium, and low risk) based on the frequency, such as every year for high risk, two years for medium, and three years for low.

## 4. *Information Required for Effective Audit of KYC/CDD*

The following information should be determined in order to evaluate the adequateness and comprehensiveness of FI's KYC/CDD policies, procedures, and processes for obtaining customer information, and to assess the value of this information in detecting, monitoring, and reporting activities:

- Understand the population of the customers.
- Use CAATs to identify red flags in customer profiles.
- Understand risk assessments that are performed from relevant audit entities.
- Review policies and procedures relevant to CDD, AML, and sanctions.
- Understand risk acceptances obtained from customers due to sanctions reasons.

- Review the enhanced due diligence procedures and processes that an FI uses to identify customers that may pose a higher risk for money laundering or terrorist financing.
- Understand approving authorities.
- Review the process of triggers for customer due diligence.
- Obtain the list of triggers from management.
- Check if there are any open issues raised in the previous audits, management self-identified issues, or third-party issues, such as regulators or external auditors.
- Understand the training requirements for customer due diligence.
- Check what governance forums are available to highlight deficiencies and red flags in KYC/CDD.
- Determine whether an FI's KYC/CDD policies, procedures, and processes are commensurate with its risk profile. Check if a bank and other financial institutions have processes in place for obtaining information at account opening and customer onboarding, in addition to ensuring that current customer information is maintained.
- Determine FI customer identification retention policy.
- Determine whether it provides guidance for documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient information or inaccurate information is obtained.

## 5. *Use of Computer-Assisted Audit Techniques*

Computer-assisted audit techniques (CAATs) or computer-assisted audit tools and techniques (CAATTs) refer to the operations of computers to automate the audit processes. CAATs generally include utilizing basic workplace productivity code, such as a computer program, word processors, written material programs, and many advanced code packages involving the use of applied math analysis and business intelligence tools.

They contain knowledge analytics routines and data processing capabilities ready to capture red flags that are a by-product of corporate executive-involvement schemes.

The most effective tools contain analytics that are mapped directly to the financial institution's core banking system. These tools are in many cases able to spot fictitious accounts, client identification anomalies, uncommon deposit activity in customer/employee accounts, cash reporting anomalies, and other red flags.

There are two broad classes of CAATs:
1. Audit software
2. Test data

## 5.1 Audit Software

Audit code is employed to interrogate a client's system. It is either pre-packaged, off-the-rack code, or it is purposely written to configure on a client's system. The best advantage of these programs is that they are customized to scrutinize huge volumes of data that might be difficult to mine manually. These programs prepare the data so the information can easily be investigated further.

Specific procedures they perform include:

- Extracting samples according to specified standards, such as:
  - random,
  - over an explicit amount,
  - below an explicit amount,
  - at certain dates;
- Calculating ratios and choosing indicators that fail to satisfy pre-defined criteria (i.e. benchmarking);
- Checking mathematics accuracy (for example additions);
- Preparing reports (budget vs. actual);
- Verifying the integrity of data (such as invoices by client or age);
- Producing letters to transmit to customers and suppliers; and
- Tracing transactions through the processing system.

These procedures will make the auditor's task easier by choosing samples for testing, characteristic risk areas, and by following certain substantive procedures. The processes do not, however, replace the requirement for the auditor's own procedures.

## 5.2 Test Data

Test knowledge involves the auditor entering "dummy" information into the client's system to make sure that the system properly mines it in a way that prevents or detects and rectifies misstatements. It aims to check the operation of application controls within the system.

To get a successful result, the dummy data should include erroneous information as well as data free from errors. For example:

- Codes that do not exist; e.g., customer, provider, and employee.
- Transactions above the pre-determined threshold; e.g., salaries above agreement amounts, credit above the threshold agreed with a customer.
- Invoices with mathematics errors.
- Submitting information with incorrect batch management totals.

Data can also be processed with a traditional operational cycle ("live" trial of data) or throughout a special run at a degree in time outside the conventional operational cycle ("dead" test of information). Each has advantages and drawbacks:

- Live tests may interfere with the operation of the system or corrupt master files/standing data;
- Dead testing avoids this situation; however, it solely offers assurance that the system works at times when not operating live. This might not reflect the strains under which the system usually operates.

## 5.3 Advantages of CAATs

CAATs permit the auditor to:

- Independently access the information kept on a computing system while not depending on the client;
- Test the credibility of client software, i.e., the IT application management (the results of which may then be utilized to assess control risk and map any audit procedures);
- Increase the accuracy of audit tests; and
- Perform audit tests more effectively, which in the long run will come up with a more cost-effective audit.

The traditional methodology of auditing permits auditors to make conclusions primarily based upon a restricted sample of a population; instead of examining the entire data or large sample of information, CAATs address these issues. CAATs analyze high volumes of data trying to find anomalies. A customized CAATs audit will not be a sample, rather an entire review of all transactions. Through customized CAATs the auditor can extract KYC/CDD details of transactions the business unit performed throughout the period reviewed. The auditor can then take a look at the data to determine whether there are any issues with the information.

# 6. Assessing the Impact of Failure of KYC/CDD on Transaction Monitoring and Sanctions Screening

Global regulations highlight KYC as fundamental to a strong AML compliance program. Without KYC/CDD, FIs cannot gather the data needed to effectively structure and build transaction-monitoring processes and comply with regulations for preventing financial crime.

A best-in-class KYC program should be one that is an ongoing process to help FIs comply with requirements and obtain continuous feedback into risk management and business strategy.

The process should be designed to ensure that you know who your customer is, what activity to expect from them, and the overall risk that the customer presents to the FI. KYC/CDD enables an FI to monitor that risk and mitigate it.

KYC can be thought of as an umbrella, under which the other items sit. A Customer Identification Program (CIP) gathers basic customer information (name, address, date of birth for an individual, and an ID number) to form a “reasonable” belief that the true identity of the customer is known.

CIP is the first phase of CDD, whereby more information is obtained regarding the individual or the entity. Things to consider could include where the individual or entity is based, whether they are a politically exposed person (PEP), the type of business they are in, or more details about their management or corporate structure.

This information helps FI determine the expected activity from that client, for example, the volume, value, and frequency of payments across an account. Transaction monitoring scenarios are set in accordance to the information gathered respectively throughout the relationship. When those thresholds are breached, the FI can seek

information about where the unusual behavior is coming from and report it to regulators if deemed suspicious.

It is clear that the entire process of transaction monitoring depends on a strong, rigorous KYC/CDD regime. The failure of an improper KYC/CDD process would cause a collapse of the transactions monitoring process, which in turn would expose the FI to financial crimes and ultimately lead to severe penalties.

## 7. Understanding Control Environment Other Than Audit

The role of internal audit is to provide independent assurance that an organisation's risk management, governance, and internal control processes are operating effectively.

The auditor has a professional duty to provide an unbiased and objective view. It must be independent of the operations auditors evaluate and report to the highest level in an organization: senior managers and governors, the compliance officer, or the audit committee.

Internal auditors can be engaged in a range of activities, which are detailed below.

- Assessing the management of risk.
- Assisting management in the improvement of internal controls.
- Evaluating controls and advising managers at all levels.
- Evaluating risks.
- Analysing operations and confirm information.
- Working with other assurance providers.

### 7.1 Regulatory Controls

Besides the activities listed above, an internal auditor should understand the controlled environments such as a specification, policy, standard, or law issued by the regulators. Regulatory compliance describes the goal that organizations aspire to achieve in their efforts to ensure that they are aware of and take steps to comply with relevant laws, policies, and regulations. Due to the growing number of AML/CFT regulations and need for operational transparency, organizations are increasingly adopting the use of consolidated and harmonized sets of compliance controls. This approach is used to ensure that all necessary governance requirements can be met without the unnecessary duplication of effort and activity from resources.

### 7.2 Self-Identified Issues

Over the years, AML compliance and auditors have heard and discussed self-identified issues, whether they should be brought to the forefront or not. AML compliance is not a single person or team activity. It will effectively yield results only when the tone is set from the top to the bottom. Frequently staff ignore or are afraid to expose self-identified issues to management, thinking that it will hit their head, but when those violations are exposed to the regulators, it damages the FI in terms of costs and reputation.

### 7.3 Compliance Review

Sometimes issues are identified during a compliance review, either by the compliance team or by the compliance officer. It is the ideal way to ensure that an FI is

implementing correct policies, processes, and procedures for the KYC/CDD process and to comply with money laundering regulations and, more important, whether the FI is adhering to the regulations.

It will help the FI in:

- Assessing whether the FI's written procedures are appropriate and being followed.
- Assessing the FI's corporate governance arrangements and effectiveness in mitigating compliance risk.
- Updating all manuals and documentation to ensure that they cover all relevant rules and regulations affecting the FI's business.
- Identifying all relevant compliance risks and ensuring that the FI has a robust system of controls in place.
- Testing the implementation of the FI's policies and procedures to ensure that controls are operating effectively and as intended.
- Reviewing the output and management information produced by the FI identify compliance risks.
- Reporting to senior management and the board on the results of the review.

Moreover, during the review the compliance team or officer will test the adequacy of the KYC/CDD program. The review will allow the compliance department endeavor to identify ways to help the practices run more efficiently, help cut down on unnecessary time and costs, and therefore improve the FI's profitability. Plus, the compliance committee will prepare a full written report on findings during the review as well as offer recommendations for improvements to the board of directors.

## *7.4 External Audit*

FIs acquire external auditors in addition to auditing their AML compliance themselves. They work independently and examine the FI's overall records and AML operations to ensure that the program is commensurate with an FI's policies and procedures. An external auditor is not affiliated with a company and thus can redirect a company's behavior without fear of repercussions. An external auditor can catch small problems before they become serious and help an FI remediate problems before regulators find issues that could be costly for the FI.

# *8. How to Test Various Elements of Customer Due Diligence*

It is important to assess various elements of CDD. For this purpose, a robust checklist is used by auditors that covers all aspects of CDD. The checklist is prepared on the basis of policies and procedures, line of business, and the walkthroughs conducted before testing controls.

A checklist ideally will cover all the rules pertaining to CDD mentioned in the policies and procedures, such as: customer risk assessment, KYC, the source of funds, source of wealth, KYC refresh based on red flags, and existing/declined clients beyond an organization's risk appetite.

When we discuss the testing of CDD elements, we are considering it from an audit or business perspective; e.g., compliance monitoring. If a client is beyond an organization's "risk appetite," the client will not be onboarded. If within the risk

appetite, audit would obtain the all the information related to CDD mentioned above and check against policies and procedures to assess that they are reasonably designed, e.g., include applicable regulatory requirements as well as internal policies/procedures, and then perform an attribute testing confirming how Customer Identification Program information is captured, KYC/CDD information required by the internal policy/procedures is obtained, etc.

If a customer was accepted that proved to be beyond an organization's risk appetite, an audit would test to discover the due diligence process that was used. The audit also should review the documentation used to approve the customer, who approved the customer, and whether the evidence used to make such decisions was retained. Also, an audit would inquire how the organization is monitoring the customer's activity, the frequency of the monitoring, etc.

Moreover, the audit not only would check how the source of funds and the source of wealth were validated by the FI and whether the sources that generated the customer's funds were legal, with sufficient tests and proof that confirm its legitimacy, but also would check the means of transfer of cash/deposits, precious metals or financial instruments deposited with a bank, focusing on the initial deposit amount and expected deposits during the business relationship.

## *9. Risk Assessment of Audit Entities Related to KYC/CDD Post Audit and Its Impact on the Frequency of Next Audit*

FI organizations need to establish an audit frequency that is right for their business. Audits can be performed monthly, quarterly, twice a year, or once a year. Crucial or high-risk processes should be audited on a more frequent basis, perhaps quarterly or twice a year; low-risk processes can be audited just once a year or every other year.

By the end of every audit performed for the AML program, the internal auditor categorizes all the auditable entities (e.g., types of products/services being offered, customer base, and geographic footprint) on risk-based merit in relation to the elements of KYC/CDD that

- Identify and verify the identity of customers;
- Identify and verify the identity of beneficial owners of legal entity customers (i.e., the natural persons who own or control legal entities);
- Understand the nature and purpose of customer relationships; and
- Conduct ongoing monitoring to maintain and update customer information and to identify and report suspicious transactions.

A risk assessment model is prepared consisting of issues with high, medium, and low risk and rated as "Matters Requiring Attention" (MRA), "Critical," or "Major or Reportable." The model will determine the frequency of the next audit (e.g., every year, every two years, or every three years).

It will form the basis of a future audit plan in which the auditor will be able to learn whether the lapses discovered during the previous audit were rectified. The auditor will be able to prepare his or her audit plan based on the assessment model where issues were mapped on a risk-based approach.

## *10. Conclusion*

The above discussion leads us to conclude that the role of internal audit is as important for auditing KYC/CDD as it is for the entire AML regime of any financial institution as well as other auditable entities of an FI. KYC/CDD plays a vital role in the development of any AML compliance program.

A sound KYC/CDD program includes strong customer acceptance, identification, and account-opening policy; it helps the FI to determine the true identity of each customer and assess the risk or potential risk presented by the customer. The process of KYC/CDD, sanctions screening, and transactions monitoring are interrelated. To acquire the desired result from sanctions screening and transaction monitoring, a robust KYC/CDD regime forms the baseline: It helps the financial institutions to uncover any unwanted customers and prevent them from penetrating the financial system before carrying out illicit activities. For effective audit of KYC/CDD, besides the FI's policies and procedures, the internal audit team must also understand the population of its customers, utilize computer-assisted audit techniques, review the business approval procedures and authority, and determine whether the bank's KYC/CDD policies, procedures, and processes are commensurate with the bank's risk profile.

Every KYC/CDD program is designed to ensure that no sanctioned or blacklisted customer enter the financial system, and that all information the FI seeks for transaction monitoring is correct and matches the criteria of the FI's KYC/CDD defined standards. If not, the entire system of sanctions screening, and transaction monitoring will be subject to collapse. To yield the desired result, the auditor can also refer to other controls that are part of the regulatory requirements; to issues identified by the FI's employees and AML compliance team; and to lapses in the KYC/CDD program uncovered by external audit.

To test the effectiveness of a KYC/CDD program, checklists are prepared that ideally cover all the rules pertaining to KYC/CDD mentioned in the policies and procedures, such as customer risk assessment, KYC, source of funds, source of wealth, KYC refresh based on red flags, and existing/declined customer that falls beyond the organization's risk appetite.

By the end of every audit process the internal auditor must establish an audit frequency of all the auditable entities in relation to the elements of KYC/CDD on a risk-based approach. It will help the FI to form the basis of a future audit plan, in which the auditor will determine which entity should be audited more frequently.

## *References*


https://www.federalregister.gov/documents/2016/05/11/2016-10567/customer-due-diligence-requirements-for-financial-institutions
https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_012.htm
https://www.fdic.gov/news/news/financial/2008/fil08038a.html
https://complyadvantage.com
https://intranet.birmingham.ac.uk/finance/internal-audit/index.aspx