Challenges in Implementing Effective AML Compliance and Internal Audit Programs in a Global Enterprise

Sid Valluri Ph.D., CAMS
Contents

INTRODUCTION .......................................................................................................................... 3

THE CHALLENGE OF COMPLEXITY ...................................................................................... 3

Country Based Risk: .................................................................................................................. 3

Variations in Experience & Training: ....................................................................................... 4

Variations in Privacy Laws: ....................................................................................................... 5

Varying Document Standards: .................................................................................................. 6

Varying Data Standards: ........................................................................................................... 6

Varying Institutional Standards: ................................................................................................ 7

Payment Type Variations: ......................................................................................................... 7

Regulatory Variations: ............................................................................................................. 7

Other Differences: .................................................................................................................... 8

COMMON PRINCIPLES PROMOTE SIMPLIFICATION............................................................. 9

HARMONIZATION DEFINED .................................................................................................. 9

THE BENEFITS OF HARMONIZATION ................................................................................... 10

A PRACTICAL APPROACH TO HARMONIZING COMPLIANCE MANAGEMENT ....................... 11

IMPACT OF HARMONIZATION ON INTERNAL AUDITS ......................................................... 12

POSTSCRIPT - NAVIGATING THE BUSINESS CHALLENGE .................................................. 13

CONCLUSION ............................................................................................................................ 16

REFERENCES ............................................................................................................................ 17
Challenges in Implementing Effective KYC Compliance and Internal Audit Programs in a Global Enterprise

**INTRODUCTION**

Global companies with multijurisdictional footprints, especially those with different lines of business, have some unique challenges in establishing, supervising and auditing an effective know your customer/anti-money laundering (KYC/AML) program. This problem is accentuated in financial services companies where a majority—or at least a significant portion of the products and services—have AML implications. Issues such as local regulatory differences, a focus on business operations, available KYC resources and geographic distance, can make the task of administering an effective program more difficult. That in turn complicates the task of the auditor who has to account for the many differences and ensure that the programs are effective, and despite their variations, faithfully follow their documented procedures.

This paper focuses on the KYC aspects of compliance programs and identifies common issues that arise. It presents a risk-based approach to streamlining them while achieving commercially compatible effectiveness.

A similar approach is applicable to other compliance areas beyond KYC/AML, but these are beyond the scope of this paper. Lastly, while this paper focuses the discussion on individual retail clients, the arguments are also valid for entity clients.

**THE CHALLENGE OF COMPLEXITY**

When a company operates in multiple geographies, complexity enters the picture in many ways. The geographic aspect may enter the picture both through the location of company operations as well as the location of the clients it serves. There are a variety of issues that emerge in such situations and the more common ones are discussed in more detail below. In later sections, we will review an approach to handling these challenges in a way that reduces complexity and benefits the business.

**Country-Based Risk:**

The primary way in which such enterprises encounter complexity is through the lens of country-based risk. This is further complicated by several key elements:

- The location of the business operations or subsidiaries
- The location of the clients being served
- The residency and citizenship of individual clients
- The location of financial institutions utilized by individual clients to fund transactions
These elements can quickly complicate the AML assessment and decision-making process. If the AML compliance group does not have well-thought-out rules that determine how various scenarios should be risk rated, the institution may open itself up to manipulation and regulatory risk. For example, an individual residing in a low-risk jurisdiction may be a citizen of a very high-risk country, or may carry multiple passports when that is allowed. The situation may be further complicated by the fact that they may legitimately own bank accounts in yet other countries with their own risk ratings. Even if a company follows standard practices and assembles a country risk rating register that reflects updated inputs from established lists such as those from FATF and Transparency International, using those ratings in specific situations can be tricky. That trickiness can lead to different decisions across the enterprise for similar situations. Therefore, the first step in being able to rationalize AML programs across the globe is to develop a country risk rating program that incorporates relevant inputs from the accepted authority sources. The second and more important step is to think through the various scenarios that will likely emerge in the course of normal business and develop clear rules on how to score them. These rules should, at a minimum, incorporate the four bullet points above in the decision logic. When there is room for variance, the compliance professional should err on the side of a higher risk score until the business can demonstrate the existence and adequacy of compensating controls that reduce the risk.

Variations in Experience and Training:
A not uncommon result of managing compliance in a global organization is a local misunderstanding of what KYC is all about. At a fundamental level, KYC is about identifying the unique individual customer, their intentions and anticipated transaction pattern, the suitability or appropriateness of the desired product or service utilized and the risk associated with providing them with those services. A good KYC assessment is intended to better enable an institution to detect and suppress inappropriate transactions.

Given the multiple layers of organization, the various lines of business and the varying qualifications and training of staff, it is not surprising to find persistent practices in local offices that resist improvement. Entrenched behaviors cause staff to spend time on non-value adding activities such as well-intended but unproductive amateur sleuthing. Beyond the time wasted, this also can lead to assessments that are not grounded in the regulations or law. When probed, the local staff often explain their approach as “We have always done it this way” or “My (local) manager wants it done this way.” Mere awareness of a different prescription in company policies is not a guarantee that employees will stand up to pressures to act differently.
Variations in Privacy Laws:

According to Privacy International\(^1\), over 100 countries have enacted comprehensive data protection legislation and many others are in the process of doing so. The organization defines personal information as:

“Any kind of information (individually or as a set) that can personally identify an individual or single them out as an individual. The obvious examples are name, address, national identification number, date of birth or a facial image. Less obvious examples are vehicle registration and plate numbers, banking card numbers, fingerprints, IP addresses, CCTV footage and health records.”

The KYC practitioner will immediately recognize that this is the very data that they are required to obtain and verify. As data protection laws vary across countries, the manner in which such information can be obtained, utilized, shared and stored also varies. Even when the required data can be acquired, global firms that need to move data across borders due to their operational, technological and organizational structures quickly run into legal barriers. For example, firms may have an accounts processing hub that serves multiple countries. This hub may be restricted in the information it is legally allowed to access or share with affiliated companies in other regions.

Broadly speaking, the EU and European Economic Area have the strongest and most comprehensive data privacy laws. While it is a hub of global commerce, the U.S. does not have a comprehensive privacy law. The U.S. Privacy Act of 1974 applies to the federal government and some subsequent laws apply to specific sectors and protect only U.S. citizens and residents.

Privacy laws are also enforced with different enthusiasm around the world. In some areas these are what one would reasonably expect in the safe handling of confidential information. However, some financial regulators have specific rules stating that, even with the same company, staff outside the regulator’s country may not have access to PII. This forces the company to have their technology systems architected so as to enable these controls. This can be a daunting task if the system design did not anticipate that need from the start. An even more draconian requirement imposed by some regulators is that PII resides within the boundaries of their country. This can be quite challenging in companies where back-office functions are concentrated in certain global locations and cross-border data access is essential. In addition, one wonders if the regulators fully understand where technology is heading. With cloud storage and cloud hosted systems becoming the norm, the actual data belonging to a company may be fragmented in globally dispersed server farms. The notion of the location of information itself is likely to get progressively more obtuse. Limitations such as these affect the ability of a KYC/AML program to streamline processes. One hopes that these issues are remedied by more uniform guidelines imposed by regulators in the future with allowance for how technology is changing the way in which business is conducted.

---

\(^1\) [www.privacyinternational.org](http://www.privacyinternational.org)
Varying Document Standards:
One of the trickier issues to handle is the variation in document standards. This refers to both the primary identity documents as well as secondary documents providing proof of address, assets or income. Even primary identification document can vary substantially across countries. Western countries like the U.S. have well established birth registries and mechanisms to provide driver’s licenses and passports. However, a single method of ID may not apply to all residents. In other places like China, a national ID card provides a unique identifier, especially in a country where there is commonality of names and the translation of names into western scripts further hinders identification. A household registry card in China is another widely held government document that complements the national ID card in establishing identity. However, that is where things get complicated. These documents are typically registered to addresses belonging to the parent of the individual as they are typically issued at maturity in the case of the ID and pertain to a piece of property in the case of the registry. Therefore, when an individual moves to a big city to pursue a career, they often do not have address documentation that one would expect elsewhere such as phone or utility bills as they are typically renters and pay in cash. Similarly mobile phones are obtained on pay as you go plans and are not registered to an address either. Bank account records may retain their parental address as they view their current address as a transient one. Therefore, KYC programs that insist on proofs of current address may run into roadblocks. In such instances, the AML officer may recognize that a combination of a national ID card and a household registry document provides a more reliable identification of the individual than attempts to validate their current transient address.

Even when documents are obtainable, such as an online banking statement, these electronic documents may be forged or photoshopped. Therefore, supplementary means of establishing source of funding account ownership, such as conducting a test deposit or payment from the provided bank or credit card account, may be needed to establish account ownership. In some instances, regulators allow the sending of an alpha-numeric code via snail mail to the address provided by the applicant. The applicant then has to call in with that code to complete the application. In this author’s opinion, that is a weak check as it merely ensures that the individual has access to mail delivered at that address or knows people living at that address. It does not in any way ensure that the individual actually lives at that address.

Varying Data Standards:
A challenge to automation and harmonization (described later in this paper) is the current variation in data standards across the world. This manifests itself in several ways:

- Even with similar rule sets, EID pass rates can vary across vendors and vary even more dramatically across regions. It is hard to determine if these variations are due to the capabilities of matching and screening algorithms used by vendors or if they are due to their underlying datasets being of differing quality.
- Significant variations exist in the information accompanying a transaction. While the originating financial institution may pass on information on the client’s identity, several
processors, especially in the charge card industry, strip out that identifying information and only transmit the amount and destination account information.

- The requirements for PCI compliance (relating to safe electronic storage and handling of sensitive information) are imposed with differing seriousness across the globe. When a transaction passes through an intermediary that is not PCI compliant, institutions further down the line lose the identifying information that was stripped at the intermediary who was not PCI compliant.

**Varying Institutional Standards:**
A benefit of the coordination across countries in the AML/CTF battle is that institutions are more aware of their obligations to combat these threats and they are progressing toward adopting common standards. This broad dissemination of standards enables companies to take comfort in, if not always rely on, the additional due diligence obligations placed on other institutions involved in the transaction. The reluctance of established multinational financial institutions to conduct business in countries with poor AML standards and poor enforcement, provides a forcing mechanism that will reduce the number of very high-risk countries over time. There will be a persistent set of countries in this group, but that is likely to be because of intentional bad actors rather than a lack of awareness of standards. At this point in time, there are still countries that participate in significant cross-border economic activity, where practices adopted for client convenience simultaneously hinder the objectives of the AML professional. For example, banks in certain Asian countries accept cash for transmittal from non-account holders. This enables fungible assets to enter the electronic funds system without the typical scrutiny or audit trail that one would expect to find.

**Payment Type Variations:**
A brief mention should be made about the expanding number of value transfer mechanisms, even when considering just currency and currency equivalents. The variety of mechanisms available to inject funds into the electronic banking system include various forms of plastic cards, e-payment methods, MSBs and virtual currency merchants, to name a few. These are frequently regulated by different regulators even within the same country and, therefore, represent a complex challenge for the AML officer when geographic variations are thrown into the mix.

**Regulatory Variations:**
Finally, a major source of variation is the approach of regulators in different regions. Many regulators take a prescriptive approach and specify in detail the minimum information needed to support good KYC and provide additional guidance on AML monitoring processes. This guidance may be further developed through the ongoing publication of interpretive notices as well as disciplinary actions which highlight the failures (and punitive consequences thereof) of firms under their supervision. In addition, detailed annual regulatory audits will examine and opine on the quality of information gathered, the data assessment mechanisms and red flag reports, and the quality of procedures, controls and supervision. Together the foregoing elements present
the company with a compendium of information and feedback. Those can and should be utilized to improve AML/CTF/KYC and compliance/risk management operations in general.

However, there are many regulators around the world who may be described as “principles based.” Rather than provide detailed prescriptions for what needs to be done, they provide higher level principles and guidance. That approach, while giving the companies the ability to tailor programs to suit their situations, also leaves them with the uncomfortable question of “Have we done enough?” In some cases, such as in the EU, independent bodies such as the Joint Money Laundering Steering Group (JMLSG) fill the gap by providing specific guidance that is then adopted, or at least endorsed, by those regulators. There are many regulators that compound this confusion by not conducting regular audits. Therefore, firms may go for an extended period of time where they are relying on their own expertise, or that of hired consultants, to assess if they have instituted competent AML/KYC programs.

Other Differences:
Regions and countries differ in many other ways in their requirements for KYC programs, such as:

- Differing standards for face-to-face contact vs. remote/online applications
- Whether new KYC requirements applied retroactively to existing clients
- Frequency with which supporting documents need to be refreshed
- Document authentication/notarization standards
- Viability of non-documentary methods for establishing identity
- Minimum transaction thresholds below which KYC is not required
- Beneficial ownership thresholds
- Availability of simplified KYC due diligence for certain classes of clients
- Requirement to report transactions other than SARs such as unusual transactions or international wires
- Requirements for systematic reporting in addition to suspicious activity reporting
- Existence of specific laws that define personal data and sensitive data and the handling thereof. These laws which include banking secrecy laws may govern not only the handling of information within the country but specify restrictions on data that may leave (or be viewed outside) national borders. Some areas have similar restrictions on inbound data.
- Requirement for a risk-based approach. These risk factors include, but are not limited to: domicile/citizenship of parties and beneficial owners, type of business, origin and destination countries for payments, type, volume and frequency of transactions, complexity of ownership structures, absence of personal contact with beneficial owners, PEPs, correspondent banking institutions, potential for anonymous activity, requirement for onsite assessment/verification for entity clients, etc.
COMMON PRINCIPLES PROMOTE SIMPLIFICATION

Clearly there are many ways in which the task of conducting an effective compliance program can quickly get overwhelming. Fortunately, at least for the AML/KYC compliance team, there are two elements that can enable a global company to have confidence that it has established a compliance and internal audit program with high standards:

1. Whether subject to a rules-based regulator or a principles-based one, the underlying concepts, principles and practices of AML/KYC are pretty universal. They are also largely common sense when one understands that the ultimate aim of these programs is to confirm that the flows of funds are from legitimate sources and in service of legitimate transactions. In order to do that, one needs to have an adequate understanding of the purpose of the account and monitor the anticipated versus actual activity in the account.

There are many organizations that work hard to improve KYC/AML and audit practices (FIU’s, Wolfsberg Group, JMLSG, ACAMS, FFIEC, etc.). They constantly build up the body of knowledge and disseminate information on money laundering typologies so as to help suppress illegitimate fund flows and their associated undesirable activities. These sources of information are readily accessible to companies around the world (though some watch lists, such as the USA PATRIOT Act Section 314(a) requests, have more restricted distribution). The universality of the principles underlying KYC/AML, makes it possible for companies to obtain and apply high quality and detailed program guidance from other regulatory regimes, even if their own regulators do not provide much information.

2. The second realization that can assist a multijurisdictional company is the new “harmonization” approach described in this paper. The logic and motivation behind the traditional risk-based approach has been to tailor KYC/AML efforts based on the risk posed by different situations. This is intended to enable limited resources to be deployed in the most effective manner possible, preferentially targeting higher risks with tighter controls, more resources and scrutiny. The remainder of this paper encourages the reader to consider resource optimization from a new viewpoint that achieves that optimization through principles-based simplification while simultaneously raising the overall bar on quality.

HARMONIZATION DEFINED

The concept of harmonization recognizes that there are more commonalities to the AML/KYC process across geographies, product lines and customer types than there are differences. When regional differences exist, they can often be resolved by harmonizing the policies in various regions by adopting the highest local standard as a uniform global standard.

These commonalities can enable a company to achieve simplification by picking the higher standard when there are variations across the world and applying that higher standard everywhere. When a program is harmonized in this manner, it has the beneficial side effect of
raising the bar in terms of standards. A company that proactively exceeds a regulators’ expectations in many areas is more likely to be treated fairly in areas that are found wanting in audits.

At first glance, this may seem like it would impose an unreasonable overhead in terms of cost and effort. In reality, the benefits of standardization are considerable. This is especially true now that many tasks are automated and it does not take additional headcount to pursue this approach in many areas. In fact, it leads to a significant opportunity to realize savings as the company no longer has to have multiple versions of policies, procedures, training programs, audit programs and update cycles. A company employing this approach will find that the program also changes less frequently in response to local changes since those changes are often just catching up to a higher standard elsewhere. Similarly, this approach reduces the need to constantly review internal training content and maintain and update multiple versions of machine-based rules. Eliminating different standards and focusing a single clearly defined approach reduces confusion among cross functional staff on which standard is applicable in which situation. It also enables more flexible staffing as local specificity is less of an issue when allocating tasks. From a senior management viewpoint, it promotes consistency in messaging on the importance of AML/KYC in good corporate citizenship.

Certainly there are limits to extent to which a program can be uniform. Despite the commonality of principles, there are local variations in rules that must be adhered to. For example, one regulator may have unique requirements for accounts opened without a face-to-face interaction. Another regulator may not allow certain kinds of documents as proof of address. These specifics have to be catered to. A practical way to do this is via a local addendum to a parent policy that calls out variations for specific areas. These addenda are typically shorter and easier to maintain and update compared to entirely separate policies. It also brings additional scrutiny to changes to the addenda that then have to be justified before changes are made. Despite the need for these adjustments, the broader simplification achievable still makes this an approach that is worth serious consideration. The benefits of harmonization are more pronounced when the company has a single or closely related business lines that have similar AML/KYC and compliance issues.

**THE BENEFITS OF HARMONIZATION**

With a few exceptions, harmonization results in less administrative overhead, fewer versions of key policies, procedures and training programs. In addition, it facilitates the creation of uniform data and analytics standards and the adoption of a common technology standard. Most importantly, it enables the company to have clear supervisory procedures and a cleaner framework from the perspective of internal and external audits.

A tangible benefit exists for those listed or regarded as supervisory management from the viewpoint of the regulators, including AML/KYC supervisors, compliance executives and board members at corporate and subsidiary levels. A harmonized program enables these individuals to
have a better chance of knowing the necessary details of, and competently performing their supervisory duties. In addition, with a harmonized program, when deficiencies are identified anywhere in the system these findings may be readily transferred across the enterprise so as to root out similar issues elsewhere—a best practices sharing approach. The author also found a significant saving of compliance time in not having to cater to wide local variations in policies and procedures that were more rooted in historical practice than differing regulatory mandates.

From both the supervisory and audit perspectives, a harmonized approach enables a simplified application of risk-based program management. Apart from the obvious benefit of not maintaining and administering multiple versions of everything, here is the real value in harmonization: When the core compliance principles, procedures and controls are largely similar across businesses, the application of the risk-based approach is manifested most in the frequency of supervisory and audit activities. In areas of higher risk (area could refer to a geography, type of client or even a type of product or transaction), the most effective control is then increasing the frequency of the assessments (more frequent assessments or larger sample sizes in audits).

A PRactical Approach to Harmonizing Compliance Management

It is this author’s experience that for a compliance operation, a top-down approach with bottom-up inputs is the most effective way to ensure consistently high standards. For this approach to work, the local entities need to have a strong awareness of their regulations and compliance responsibilities and be held accountable through appropriate supervision and reporting procedures.

The first step in a harmonization exercise is clear direction from the senior compliance executive on the goal of reducing complexity and raising standards. The following broad steps will facilitate a viable process after the necessary stakeholders have been identified and included:

1. Catalog key policies and procedures and assemble copies of all variants.
2. Identify the most comprehensive version of each document type (the Master). Assign responsibility to a competent professional from each region to review their local document against the Master and note key differences with the Master. In particular:
   a. Areas where the Master is the higher standard
   b. Areas where the local document is the higher standard
   c. Areas where the two are incompatible
3. Circulate a revised Master and incorporate into it the higher local standards, where applicable. In practice this will require several rounds of reviews and edits.
4. Collate areas of incompatibility and review in a conference call with stakeholders (email is an ineffective collaboration tool). When highly specific or incompatible criteria emerge that cannot be harmonized, incorporate these as local addenda to a global document.
5. Repeat this process for procedures, assessments, controls and training programs.
6. Outline an update process:
a. How frequently will the documents be updated?
b. How are update requests captured and acted upon?
c. Who will decide when a change request will be implemented as a local variation vs. a global change?

Use of an online collaboration tool that enables comments and version control accelerates this process. In addition, it is invaluable to have a tool that captures explicit sign-offs from key stakeholders. This confirms that all necessary have been received and also binds the individual to the final result.

It is essential that the local compliance experts from every region and business line review and comment on the policy with the aim of finding a common standard. This approach will likely meet initial resistance, but persistence on the part of the senior management will achieve the necessary inputs. Unfortunately, one feature of this approach is the requirement to have several rounds of review on each policy. This is necessary because changes made in a prior round may have new regulatory implications in a different region thereby requiring another round of input.

**Impact of Harmonization on Internal Audits**

While the harmonization process is applied to the compliance program itself, the simplification that results simplifies the design and execution of the internal audit. For example:

**Full review of Program Manual**

- Time savings from significantly reduced volume of policies and procedures
- Fewer updates/changes from prior years
- Focus time on whether the policies, procedures and controls adequately assess and address the risks associated with the business

**Testing of Policies and Procedures**

With more uniform policies and training, aberrations are easier to detect. Peer-to-peer coaching also enhances compliance by personnel. Note that when failures do repeat they are likely to be systemic (i.e., prevalent widely) and from two causes: 1) Inadequacy of some program element and 2) Poor individual performance. In the case of the latter, additional samples from that individual should be tested. Systemic failures need to be escalated for remediation promptly, possibly even before the audit concludes.

**CIP Review**

This is one area where firms can have wide variations in policies, documentation needs and approval standards. Harmonization to a single standard with minimal variations should simplify the task of the auditor considerably.

**Transaction testing and evaluation**
Depending on the types of transactions handled by the institution, this may or may not be an area amenable to harmonization. However, if a firm uses a common information architecture, then at least the rule sets and use cases programmed into transaction monitoring systems can be reviewed for consistency of their logic and thresholds/filtering criteria.

The other areas that audits touch on such as OFAC/sanctions compliance checks, mandatory filing reviews (SARs, CTRs, etc.), MIS evaluations and assessments of past audits are less likely to be impacted by a harmonization effort.

While a harmonized approach supports more effective internal audits, companies should be aware of the maxim “We don’t know what we don’t know.” Even with the best intentions, an internal audit program will likely repeat the examination protocol of prior periods with incremental improvements. It is for this reason that the regular use of external auditors and consultants is recommended. An external review would complement the work of the internal quality assurance team in the internal audit department and peer reviews within the audit department itself.

**POSTSCRIPT - Navigating the Business Challenge**

A compliance group exists within a larger organization that seeks to sell products and services and derive a profit. A key challenge to the senior compliance executive is maintaining a balance between effective regulatory supervision and enabling the business to operate effectively. Despite its legal and regulatory mandate, a compliance team is not likely to be regarded as a welcome presence or influence. Along with other staff functions such as HR, finance and legal, it is often seen as imposed overhead to be endured, rather than a value-adding element of the business. With that framing, it is often challenging to acquire the necessary budgetary support and leadership buy-in.

Undoubtedly, a C-level role for risk and compliance is a valuable way of getting the necessary voice and visibility in the organization, especially if a direct report to the Audit and Risk Committee of the board is a part of the organizational design. However, that is just the start. That C-level executive will still be faced with a battle to demonstrate the ‘value add’ of the compliance organization. In many organizations, that task is further complicated by other senior business leaders complaining about the obstruction, overreach or burden placed on their ambitions by an overzealous internal policeman. Indeed, as many of those in the risk and compliance fields come from legal or analytical backgrounds, there is an understandable tendency to focus on the letter of the law rather than the business goals. For many it is hard to make the mental shift from “This isn’t permissible as it violates the regulations” to “How can we achieve what the business is trying to achieve in a compliant and ethical manner.”

Compliance can and should be seen as an asset to the business. Instead of being the beat cop that merely issues tickets for infractions, it can take an active role in educating the business on
regulatory objectives while identifying opportunities to streamline and improve operations in a manner that is consistent with laws, regulations and professional ethics.

Especially in the context of multiline global businesses, such proactive assistance brings immediate benefits. When policies worldwide are reviewed and revised with business knowledge, common sense and clarity in mind, the business operations achieve improvements that are measurable in days and weeks rather than years. This review needs to be done by a team that has a strong basis in compliance while having a thorough understanding and appreciation for what the underlying business is trying to accomplish. A well architected compliance program, especially with AML/KYC objectives in the forefront, can in fact enable the business to operate more smoothly and productively. A brand that is recognized by customers and regulators as being principled, fair and ethical will reap the economic benefits of customer loyalty.

While a harmonization program alone will demonstrate measurable economic benefits, such a program implemented with input from and cooperation with the business will produce far greater rewards. In particular this proactive partnership can be achieved through activities such as:

- **Reviewing the compliance policies to make sure they are up-to-date and reflect the current regulatory environment.** For example, historical policies requiring duplicate or triplicate documentation may still persist. These are of course redundant with the wide availability of information systems that make the information accessible to all who need it. In other areas, technology has made prior practices questionable. An example of this is the ‘maker-checker’ model of reviewing client applications. In this model, one employee reviews the application and accompanying KYC documentation and another performs exactly the same task to ensure that it is properly done. The ostensible reason for this duplication is that compliance or AML regulations require this approach. It also supposedly ensures that any bias or conflict present in one individual will be neutralized by the second check. With methods such as EID (electronic identification) supplementing KYC checks, continuing this approach actually results in a slower account approval process and a wasted headcount without any measurable benefit in terms of quality. When an individual performs a task, and knows that another individual has or will repeat the task, human nature indicates that one or both of them will perform the task less rigorously. This is natural as they expect that any mistakes will be caught by the other and therefore the bar on failure is lower. A better approach would be to ensure that the individual is well trained and increase the level of spot checking based on the applicant’s risk score. Customer profiles with higher risk scores (based on whatever set of metrics the organization applies), should be spot checked with higher frequency than those with lower risk scores. This does not reduce the necessity of supervisory approval of new accounts as that is mandatory in many jurisdictions. When the spot checking is done by an independent group, possibly by members of the internal governance group or audit
group, it operationalizes one of the four key pillars of effective AML—
independent testing and verification.

- **Reviewing business practices and employee training to ensure that they reflect a strong knowledge of the relevant current regulations rather than entrenched legacy practices.** This is especially important when the staff performing these tasks have little interaction with compliance and regulatory staff and perform their duties based on what others in similar roles do.

In roles relating to KYC, it is not uncommon to find staff investigating suspicions with the zeal of an amateur detective. When there is a well-founded cause for suspicion, it is the obligation of an AML staffer to carefully assess the situation. However, when this obligation is misunderstood it can lead to a significant waste of time and process delays when the sleuthing becomes recreational or zealous in nature. A disguised example of this is an AML staffer initiating an investigation because a brokerage applicant listed ‘Shanghai Trading Company’ as their employer but listed an address in Beijing. The employee decided this was suspicious. When multiple Google hits were returned for names of similar companies in China, the staffer began to investigate the various companies for their office locations. The staffer failed to realize that the reason the employer information was required was to determine the client’s principal occupation or business so as to gauge their risk tolerance and the suitability of a speculative trading account for the client. This misunderstanding led to a waste of time and unnecessary delays.

- **Providing the business with advance warning of upcoming regulations** along with insights on how the business may adapt to those changes, or better still take advantage of them.

- **Utilizing regulatory mandates to acquire the necessary budget and resources to support particular business goals.** For example, in the U.S., the CFTC recently approved regulations requiring firms to have a comprehensive approach to information security and risk management. Investments in these areas tend to demonstrate their value over the longer term or in crises. As a result, they also tend to be under resourced relative to shorter term revenue generating initiatives despite their intrinsic value and longer term payoff. When the compliance function realizes that they can advocate for such business enhancing investments based on regulatory mandates, they reap the benefits of being seen as a partner to the groups needing these resources rather than a policeman.

- **Reducing losses, fraud and wasted resources from poorly screened clients.** A proper risk-based evaluation of a client is conducted with an eye towards understanding the nature and frequency of expected transactions as well as the business intent behind those transactions. When this assessment throws up valid red flags, it helps screen out clients who eventually cost the business money rather than bring in profits. On the flip side, this requires the compliance professional to invest time in developing an intimate
understanding of the business. This enables them to tune the red flags to catch suspicious issues while minimizing false positives.

- **Collecting cross functional viewpoints** – Internal audit teams get a broader and deeper view of the business than most employees. They have the obligation and opportunity to ask probing questions and to understand the business and its risks from a unique perspective. This simultaneously enables them to identify risks and opportunities that may be missed by others who are more narrowly focused.

To be clear, it is not always possible to find a constructive or alternate solution. Also, there are plenty of times where individuals or organizations lose sight of regulatory principles and have to be firmly reined in. In other instances, competing demands and lax supervisory oversight may result in violations from inattention. Ensuring that the business stays between the lines is the purpose of clear policies, strong supervisory oversight and an effective internal audit program. However, when the compliance group is also seen as a supportive partner, the benefits are apparent and lasting.

**CONCLUSION**

Complexity in AML/KYC operations arises from many sources. When operations are global, the sources of such complexity multiply rapidly. The compliance team is required to be aware of and manage the differing demands of regulators around the world and that results in an explosion of largely similar, yet different policies and procedures. The task of maintaining this variety is expensive and time consuming. When the harmonization approach described in this paper is implemented, it reduces the workload on compliance resources.

Because a harmonization exercise implies a top-down control environment, it makes more visible attempts to change policies and procedures and fosters the creation of an audit trail documenting the source and motivation for proposed changes. This acts as a natural defense against diluting standards, especially for commercial reasons.

When unnecessary differences and complexities are removed from policies and procedures, it makes the task of the auditor simpler. Before a harmonization exercise, an audit group would need to invest time in collecting and reviewing various versions of each policy and then verifying that the supervision and controls were appropriately set up to ensure their effectiveness. Then it would need to devise and conduct the tests necessary to validate those controls and the training programs that support these policies. With a reduced variety of these policies and controls brought about by harmonization, the auditor can achieve a higher degree of assurance with the same sample size. Alternatively, they may select fewer samples to reach to same confidence level.

As noted above, when the policies and standards are relatively uniform, the appropriate high-risk response is performing the necessary verifications with a higher frequency. This has an interesting implication for the auditor—they can verify the effectiveness of a high-risk control by
reviewing the rate at which higher risk clients were assessed rather than having to specifically review those assessments themselves.

As this paper proposes a new approach to architecting a compliance program, there is a need for a body of practice to evaluate the appropriate audit approach over time. Initially at least, it will be prudent to follow existing audit protocols. Over time, auditors will discover that some tasks are unnecessarily repetitive in a harmonized environment and will simplify procedures accordingly.

REFERENCES

1. Anti-Money Laundering: 5 Steps to Conduct an Audit; Larry Schneider, New York Institute of Finance
2. Know Your Customer: Quick Reference Guide. PWC. www.pwc.co.uk
5. Joint Money Laundering Steering Group (JMLSG) (http://www.jmlsg.org.uk/)