Deloitte.

Meeting new expectations

Foundational considerations when upgrading Know Your Customer programs

Deloitte Center *for* Financial Services

Contents

"The inadequacy or absence of KYC standards can subject banks to serious customer and counterparty risks.

[Yet] the implementation and assessment of KYC standards tests the willingness of supervisors to cooperate with each other in a very practical way, as well as the ability of banks to control risks on a groupwide basis.

This is a challenging task for banks and supervisors alike.[1]"

— Bank for International Settlements, 2001

KYC: Heightened expectations, continued importance

The importance of and operational challenges associated with KYC programs are nothing new as demonstrated by the foregoing statement from the Bank for International Settlements in 2001.[1] Thirteen years later, more sophisticated money laundering techniques, new global currencies, continued terrorist activity, major fraud schemes, increasing cyber threats, and new products with greater speed of funds movement and anonymity have made KYC an even more daunting, yet no less critical task. Many of these forces have helped redefine industry standards for an effective KYC program since the Bank for International Settlements issued its statement.

These new expectations are evident in recent regulatory guidance and enforcement actions and broadly require banks to put in place measures to drive:

- Consistency in KYC standards, client risk assessment, due diligence programs, and decision-making
- More effective KYC data management, including improved data quality and aggregation of customer data across accounts and businesses to create a firm-wide view when warranted
- Line of business accountability for knowing their customers and owning the "first line of defense"

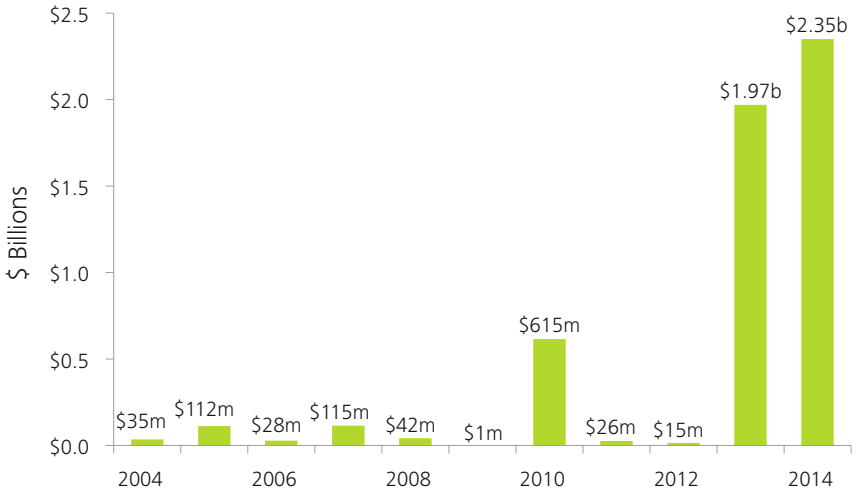
As an indicator of regulatory resolve in this space, anti-money laundering (AML) and sanctions-related fines and penalties imposed in 2013 and 2014 quadrupled the total for the previous nine years combined. (See Figure 1.)[2]

From an AML perspective, a KYC program is designed to achieve multiple objectives:

- Identify the customer and verify the customer's identity
- Understand the customer's profile and associated money laundering risks
- Assign a risk rating to the customer
- Allow the bank to perform additional due diligence on higher risk customers, conduct ongoing monitoring of customer risk, and renew due diligence based on changes and activity that is different than expected
- Make informed decisions about customers based on perceived risks

Ideally, the creation of the customer profile to identify risk has a direct bearing on a bank's ability to become more "risk aware" by improving its ability to understand what is usual and expected for the customer, apply accurate levels of controls and due diligence to its customer base, keep "bad actors" out of the bank, and focus resources on higher risk customers.

Figure 1 — Fines for AML and sanctions-related regulatory actions have increased



Source: Deloitte analysis as of January 2014

1 "Customer Due Diligence for Banks," Basel Committee on Banking Supervision, Bank for International Settlements, October 2001, http://www.bis.org/publ/bcbs77.pdf.

2 "BSA/AML Monetary Penalties List," Bankers Online, accessed June 26, 2014, http://www.bankersonline.com/security/bsapenaltylist.html.

Dimensions of a broad KYC program

Financial industry regulators expect banks to demonstrate that they understand their customer base and have considered the associated risk for their customers. For example, banks are expected to create a profile of the customer for managing risk, and not just for the purpose of assembling documentation. They should also be able to analyze the information obtained about their customers for consistency, reasonableness, and new relationship development, and compare what is known about the customer at onboarding against how the customer is utilizing the relationship. Finally, the regulators expect more consistent KYC standards across the institution and an enterprise-view of the customer rather than multiple views in the separate business lines or geographies in which the customer may transact business.

Expectations such as those cited above are documented in a multifaceted set of KYC regulatory frameworks and guidance. International standards can be found in the Financial Action Task Force and Basel Committee on Banking Supervision, Bank for International Settlements; laws and regulations in the Bank Secrecy Act and USA PATRIOT Act; regulatory notices and guidelines in the Federal Register, e.g., the Financial Crimes Enforcement Network's (FinCEN's) recent Advance Notice of Proposed Rulemaking on Beneficial Ownership (July 2014), and on FinCEN's website; and exam and industry guidance in the FFIEC BSA Examination Manual and the Wolfsberg Group guidance.

More than simply being a compliance requirement, KYC is an essential tool in identifying, understanding, and mitigating money laundering and other risks posed by customers. Thus, in order to meet today's heightened KYC compliance expectations and better mitigate financial crime risks, many banks are (or should be) reassessing and transforming their KYC programs.

The importance of KYC is clear; however, it remains a challenge for many banks to transform or redesign their KYC programs to become more effective, consistent, and efficient to satisfy today's regulatory expectations without placing significant strain on business, compliance, and technology resources, or impacting the customer experience. The breadth, number, and complexity of KYC processes and legacy bank systems can make this an overwhelming task. Further, the details and functionality of a broad KYC program will vary for each bank given both its money laundering risk exposure and customer profile, as well as its product scope, size, and complexity.

To help financial institutions of all sizes think about how they might enhance and transform their KYC programs, in this document we present seven dimensions that together could assist banks in meeting today's heightened standards (see Figure 2).

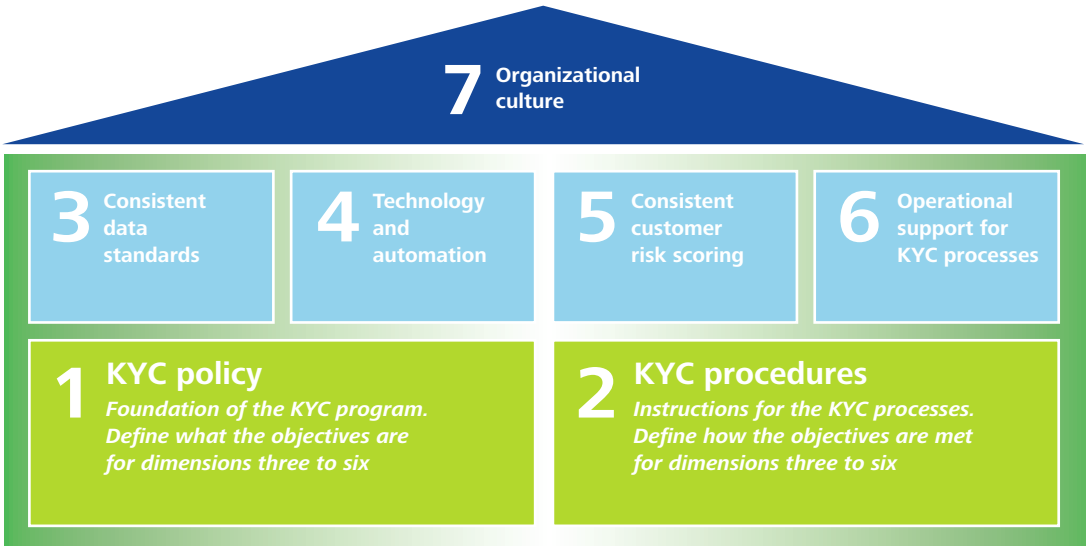
KYC dimensions

Together, all seven dimensions can help create a more effective and efficient KYC program that is designed to mitigate money laundering risks across the institution.

While each of the seven elements is important, KYC policies and procedures form the foundation for a more successful KYC program and the other dimensions build upon this foundation, culminating in a "KYC-aware" culture that is designed to bring greater organizational focus to the effort.

In the remainder of this document, we will explore each dimension and its importance, common vulnerabilities that have recently emerged, and suggested steps banks can take to address these vulnerabilities as part of a bank's KYC program evolution.

Figure 2 — Dimensions of a broad KYC program



Key characteristics

Comprehensive – Address all customer types, products, and business lines
Consistent – Apply KYC guidance across the entire enterprise
Detailed – Include clear and thorough guidance, leaving no ambiguity
Quality-focused – Deliver accurate and thorough analysis

1	**KYC policy** – the foundation of the KYC program that defines what the objectives are
2	**KYC procedures** – instructions for all KYC processes that define how the objectives are met, e.g., customer identification and verification, customer due diligence, and enhanced due diligence
3	**Consistent data standards** – the governing principles for collecting, storing, and analyzing data
4	**Technology and automation** – the integrated technology ecosystem needed to develop and sustain an effective and efficient KYC program and to help identify higher risk customers
5	**Customer risk scoring** – the quantified risk-based assessment of each customer
6	**Operational support for KYC processes** – techniques to centralize certain essential KYC activities to apply greater expertise while driving improved efficiency
7	**Organizational culture** – the appreciation of and support for KYC as a valuable compliance and risk management activity

1 KYC policy

Importance

The AML policy serves as the foundation of a sound KYC program. As the governing document for the program, the policy defines the standards, risk appetite, expectations for the organization, and what the KYC program aims to achieve. The KYC policy should describe all the relevant KYC requirements needed to both onboard and maintain customers.

Policies that either fail to capture all of the KYC activities or do not fully address current regulatory requirements could jeopardize a bank's AML and risk management efforts. For instance, regulators recently cited a KYC program whose guidance was based on the bank's legal counsel drafted in 2004. This policy unlikely reflects all the current day risk that the bank could face and may result in gaps needed for both customer onboarding and storage of required customer data.

Common vulnerabilities and suggested actions

To meet heightened expectations, banks must periodically reassess and enhance their KYC policy to ensure it meets or exceeds current regulatory expectations and is commensurate with the bank's AML and risk profile. It should include clear accountability and describe major KYC requirements for customer acceptance, identification, and standard and enhanced due diligence.

Some of the more important vulnerabilities with regard to KYC policy that have emerged recently, along with some suggested action steps that banks should consider, include:

1. When determining KYC policy and standards, the feasibility of implementation and impacts on the business have not always been considered. In some cases, policy development or updates may not be fully or accurately understood by business and operations functions. Additionally, system limitations or process and data collection changes have had, and can have significant business impact.

   Suggested action steps: AML compliance program leaders should take the step of engaging with their counterparts in the business lines to understand the feasibility of implementing KYC policy statements or revisions. For example, banks should consider how their KYC requirements at onboarding fit with other elements of the account opening process. Additionally, those responsible for updating and implementing KYC programs should determine a range of potential implementation options and develop a rollout schedule to ensure alignment with policy requirements.

2. Recent commentary from various regulators has highlighted some important cultural issues that cover KYC policies and beyond. We will touch on some of these issues later, but as applied to KYC policy in particular, it has been observed that some banks lack a common organizational understanding of KYC policy requirements.

Suggested action steps: As part of a KYC program development or update, AML compliance program leaders should incorporate time to review the KYC policy requirements with business and operational teams to ensure that a common understanding of the policy exists across the organization. Furthermore, the KYC policy should define the appropriate balance between risk management and business objectives. Firms should ensure regulatory expectations, and their own internal risk goals can be fulfilled without unnecessarily negatively impacting customer experience or passing on sound business opportunities where risks are known and mitigated.

Key considerations

Depending on the specifics of the business and the makeup of the client base, other key questions that may apply to some institutions include the following:

- How do banks ensure that the policy addresses all possible scenarios?
- Is the bank applying the same level of due diligence to customers with the same AML risk profile?
- Are adequate controls in place to ensure the policy is reviewed and updated on a regular basis?
- How are KYC standards by client type integrated into the policy framework?
- What level of prescriptive detail is best?
- Should banks define standards down to the data field level to drive consistent behavior?
- How many client types should be identified for the organization?

2 KYC procedures

Importance

While the KYC policy describes what the KYC requirements and objectives are, the procedures detail how each requirement and objective is met. Procedures are the bank staff's step-by-step instructions for collecting and analyzing KYC information.

Procedures that are outdated, inconsistent across business lines, or lack sufficient detail can jeopardize the effectiveness of the KYC program and subject the bank to regulatory scrutiny.

Common vulnerabilities and suggested actions

Regulators expect procedures to encompass all activities throughout the KYC lifecycle, including onboarding, trigger events (e.g., material changes to the customer profile, changes in the customer risk rating, and changes to the customer product usage profile), scheduled reviews for higher risk customers, and account closings.

Procedures should be consistently applied across the entire enterprise for a KYC program to be effective. In some cases, local regulatory standards, delivery channels, or client types may require customization of KYC procedures. For instance, account opening processes may differ across online, call center, and branch channels; however, banks should ensure that the customized procedures feed seamlessly into other processes without undermining the reliability of KYC analysis. Recent vulnerabilities have been identified with regard to adequate process documentation and global versus local procedures:

1. There can be inconsistencies regarding the availability of detailed process documentation in order to familiarize employees with KYC requirements and explain the need for collection of incremental customer information.

   Suggested action steps: Financial institutions should prioritize the process and procedure development effort as basic to their KYC program. Further, they should focus on providing business and operational employees with details on key changes and new additions based on policy (e.g., escalation paths or approval grids). Finally, a defined timeline should be established to address changes in policy or business rules.

2. For banks with an international footprint, globally developed procedures are typically at a higher level of detail and may not capture local (in-country) requirements and business needs. This can create challenges, as the practice of utilizing global procedures for local activities does not allow front- or back-office staff to understand activities in a sufficient level of detail.

   Suggested action steps: For banks with a more global footprint or customer base, procedures and processes should leverage global procedures; however, they should also be localized to address in-country rules and regulations, such as language localization or customization to local business practices.

Key considerations

Outside of the issues covered above, those responsible for implementing or updating KYC processes within their institutions should ask themselves the following questions:

- Although different geographies have different procedures, do they follow a similar core procedure?
- Has a process been developed for maintaining and updating procedures on a periodic basis to reflect new regulatory or policy changes?
- Are there controls to ensure AML risk management is monitored during and after onboarding?
- Has a review process been considered and how are these procedures incorporated into the KYC training sessions?

3 Consistent data standards

Importance

Data standards define the input required to accurately determine the customer risk classification and execute the necessary due diligence that is outlined in the KYC policy. Consistent, high-quality data can greatly enhance the underlying value of the KYC analysis, whereas unreliable data can jeopardize the effectiveness and usefulness of KYC information altogether.

With that said, an increased volume of data coming from a range of products, business lines, and geographies creates a number of challenges. For example, increasing volumes of transactions, and the data associated with those transactions, can negatively affect a bank's transaction monitoring capabilities if the processes and systems are not scaled to handle this growth.

Common vulnerabilities and suggested actions

Heightened KYC expectations require banks to revisit data governance programs to address common issues. For this reason, regulators appear to be seeking a much more advanced and reasoned approach to data management and governance than ever before. Inconsistencies in the way business lines capture KYC information can undermine accuracy and risk management. A lack of sufficient data usage controls can lead to gaps in customer profile information, thereby decreasing the ability to adequately detect and evaluate potential money laundering or other suspicious activity.

In reviewing data standards, banks should consider consistent definitions as well as standards for storage and proper use. Recent regulatory findings with regard to KYC data standards include the following:

1. In some cases, financial institutions may lack a unique customer identifier that can be used across lines of business and geographies as part of their KYC/AML ecosystem.

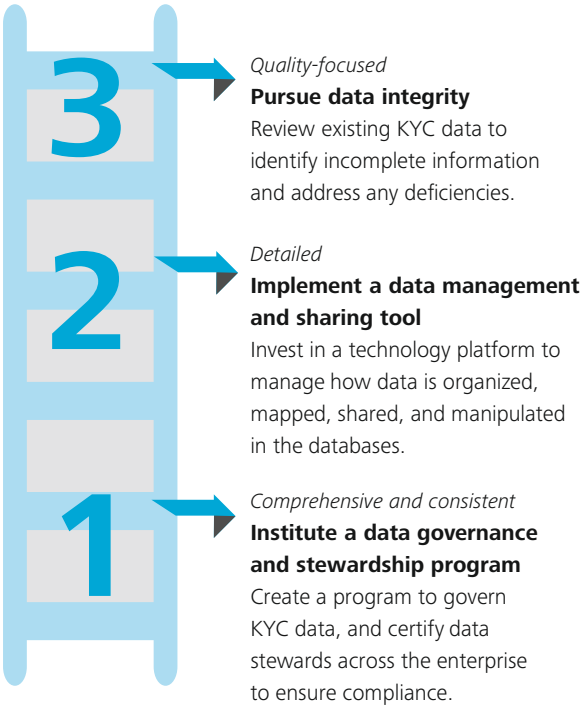
   Suggested action steps: To counteract the problem of customer record duplication, firms should adopt a single customer identifier across any and all impacted systems containing those customer records. Unique enterprise-wide identifiers can prevent duplicate data from being entered into the system and reduce the need to reconcile data errors, typically a costly and time consuming exercise. This may require changes to multiple systems feeding into the KYC platform. Additional effort should be made to eliminate duplicate records that might impact overall data integrity.

2. Similar to the vulnerability described above, some banks may have a limited understanding of customer data across business lines or geographies; for example, the number of customer records that have all risk scoring fields populated.

   Suggested action steps: The focus here should be to identify and clean up inconsistent data for key risk scoring elements. It is important to note that these data cleanup activities need to be initiated in the source systems of record mentioned above, versus the KYC system itself.

The steps above could also be supplemented by additional steps to support the development of more mature KYC data standards, namely, instituting a data governance and stewardship program, implementing a master data management and sharing tool, and creating a program to pursue data quality overall on a go-forward basis.

Figure 3 — Steps to mature KYC data and quality standards



Key considerations

As firms begin the journey toward establishing more rigorous KYC data standards, business and technology leaders should contemplate the following as part of their planning effort:

- Is data consistent across all business lines?
- What investments need to be made to improve data quality?
- How does one ensure data integrity across different systems?
- Has there been clear identification of the system of record for key data elements?
- How does one identify each customer across different systems?
- How does one de-duplicate records?

4 Technology and automation

Importance

As KYC processes grow in number and complexity, technology and automation provide the efficiencies needed to make programs more consistent and sustainable. For instance, meeting regulatory expectations for near real-time analyses to potentially detect and prevent fraudulent activities will depend on a bank's ability to properly leverage technology.

Technology solutions can be used to help banks address challenges in a number of areas within their KYC programs, including:

- Duplicate processes or inefficient workflows
- Lack of a single repository for KYC data
- Inconsistent or inadequate data privacy controls
- Lax data management protocols

Modern systems and software applications can help efficiently capture, store, share, and analyze KYC data with limited disruption to the business lines.

Common vulnerabilities and suggested actions

As KYC data collection may be a client-facing activity, reliable and fast technology is necessary. Technology that proves unreliable and time consuming can jeopardize customer service, reputation, and ultimately growth. From an operations perspective, technology should support real-time sharing of KYC data across onboarding, KYC, and customer review systems in order to effectively and efficiently mitigate risks. Robust integration with onboarding systems and tools for data migration is an essential element of a robust KYC technology architecture.

As might be expected, given the importance of data analysis to a thriving KYC program, regulatory and internal examinations have focused on the degree of flexibility, responsiveness, and integration of customer and transaction processing applications. Indeed, meeting regulators' expectations for more advanced, preemptive analysis will likely depend on a financial institution's ability to properly leverage its technology platforms.

Some common technology vulnerabilities and suggested action steps to address them include:

1. The level of integration between KYC and customer onboarding systems may be lacking in some financial institutions, leading to added vulnerabilities when establishing a new customer relationship. Oftentimes, the focus on integration has taken a back seat within the process of updating KYC technology programs in favor of developing the actual KYC application technologies themselves.

   Suggested action steps: When implementing new or upgraded KYC systems, the project team should develop detailed data mapping from the client onboarding system as well as the KYC system to ensure consistency. Furthermore, multiple mock conversions should be conducted to ensure the quality of integration and data transfer between these applications. Finally, business users should be involved early in the project to approve data transformation as data is migrated to the new platform.

2. There may be weaknesses regarding the flexibility of KYC program applications to handle the increasing complexity of client interactions across products and geographies. Additionally, to keep pace with and stay ahead of evolving expectations from regulators, KYC technology solutions should allow for configuration changes in response to new and emerging risks.

Suggested action steps: KYC technology applications should have the flexibility to be properly configured across the lines of business and geographies of the bank. The ability to reflect unique workflow steps, client-types, and risk ratings for each business line will help create a more effective KYC program. Banks can achieve this by developing and/or implementing technology that allows business lines to customize the order of KYC data collection and prioritize the type of KYC data being collected. Of course, when operating across multiple geographies, data privacy regulations must be considered.

Key considerations

In implementing technologies that support more efficient management of KYC activities, technology leaders should consider the following questions:

- Is an "off-the-shelf" solution sufficient, or does the institution's complexity require a custom technology platform?
- Does technology allow for real-time KYC checks during onboarding or is a "day two" process needed as part of the KYC implementation?
- Has an enterprise solution been contemplated that allows KYC information to be captured across business and geographies?
- Have sufficient mock data conversions been planned to test the migration of data correctly from onboarding platforms to the KYC system?

5 Customer risk scoring

Importance

Customer risk scoring helps a bank to quantifiably understand the inherent money laundering risks posed by its customers and make more informed decisions about customer risk exposures. Risk scoring may also leverage KYC and transactional (expected or actual) data and helps the bank stay within its acceptable risk tolerances.

While challenging, developing a well-defined and accurate scoring methodology allows banks to better measure and reduce money laundering exposures, develop and implement corresponding risk mitigating controls, prioritize issues, allocate resources, and manage customer risk.

Common vulnerabilities and suggested actions

A risk scoring model should be applied in a consistent manner across the customer base and reflect each institution's risk profile, size, products, and geographies. A customer's risk score should drive ongoing KYC review cycles and be taken into account in the bank's transaction monitoring program.

A broad ranking methodology considers an array of factors. These include, but are not limited to, customer segment risks (such as politically exposed persons, casinos, and money service businesses), product and transactional risks (for example, international wires or cash-intensive transactions that exceed a defined percentile of number and/or aggregate dollar value versus peers), and geographic risk (which includes not only location, but also citizenship status and expected transactional geographies).

The model should be validated to ensure its design meets both regulatory and business needs; the technology is adequate to support the risk scoring model; the data is being collected, reviewed, and stored properly; and the risk scoring process correctly rates customers.

Emerging challenges with respect to risk scoring models include:

1. Determining the appropriate number of risk categories (e.g., high versus neutral; high, medium, and low) in order to appropriately segment the customer base.

   Suggested action steps: KYC program leaders and staff should seek to work collaboratively with compliance and business counterparts to determine the categories of high-risk customers and the impact to the business. Further segmentation may be needed in some cases. Additionally, feedback loops should be integrated into the process so that changes in risk classifications are reflected in other KYC processes, as a change in the risk classification may impact how the bank monitors that specific customer.

2. As mentioned above, customer data can be fragmented and is often incomplete. From a risk scoring perspective, scoring models may lack an enterprise view of the customer as well; missing details can encompass key elements such as demographic, product, transactional, and geographic profiles.

   Suggested action steps: Risk scoring should be performed based on a customer's complete enterprise-wide profile in order to provide greater transparency regarding actual and potential risks. The scoring methodology should be comprehensive, taking measure of all business units, customer types, and available data.

Key considerations

Those responsible for risk scoring should take into account the following considerations in the process of updating their models:

- How many factors should be employed to calculate risk?
- What factors can be consistently collected across all geographies for the client types identified in the policy?
- What would be the specific weights of the different factors?
- What customer demographic input does not have a data field and will need to be derived?
- Would further differentiation of risk classifications (e.g., high, medium, and low) be useful?
- How should the client risk scoring model be calibrated and validated on an ongoing basis in accordance with regulatory requirements?

6 Operational support for KYC processes

Importance

Banks may be able to create a more effective and efficient KYC program by using operational support units for standardized or straightforward tasks such as upfront customer identity confirmation, name screening, and client outreach. Operational support units are typically centralized, noncustomer facing groups that complete some KYC processes for the front-line staff during onboarding and/or periodic reviews. One can think of a KYC operational support unit as a cadre of KYC experts who focus almost exclusively on KYC, while frontline relationship managers focus on a wider variety of activities. Creating this center of KYC expertise can increase both effectiveness (e.g., fewer mistakes) and increase efficiency.

While they may not be appropriate for every bank, larger institutions may have the specialization and economy of scale needed to make such units an efficient way to complete KYC processes.

Common vulnerabilities and suggested actions

One of the most common pitfalls in establishing operational support units is misjudging the balance between what can be centralized versus what needs to be owned by the frontline business. Establishing clearly defined criteria regarding the support units expertise may help properly pair KYC activities with support units that can complete the process in a high-quality manner. Furthermore, support units should have clearly defined roles that do not replace the business line's responsibility for understanding their customer's risk, i.e., they are helpful at providing support, but cannot replace the business line's understanding and acceptance of customers' risk profiles. With regard to vulnerabilities in this area, recent findings include:

1. Often, front-office staff may not be able to collect and validate all required KYC information during the process of initial customer onboarding.

   Suggested action steps: KYC and business teams can partner to identify the needed KYC process steps that can be completed after a client visit by nonclient facing individuals and performed through a back-office function. Of course, financial institutions should consider if they have the scale necessary for support units and if centralized processes make sense for their structure. From there, a set of activities more appropriate for centralization (e.g., research and initial name screening against government watch lists and databases) may be selected. Finally, firms should consider phasing them in from their existing locations to a support unit to allow for learning and process improvement. Gradual up-skilling of the operational staff will allow for increasingly complex activities to be centralized and customized, based on the institution's complexity and culture (see Figure 4).

2. Some banks neglect to include a feedback loop to the operational support unit that includes the results or output of transaction monitoring in KYC periodic or event-driven reviews. Such information may cause a change in the customer risk rating.

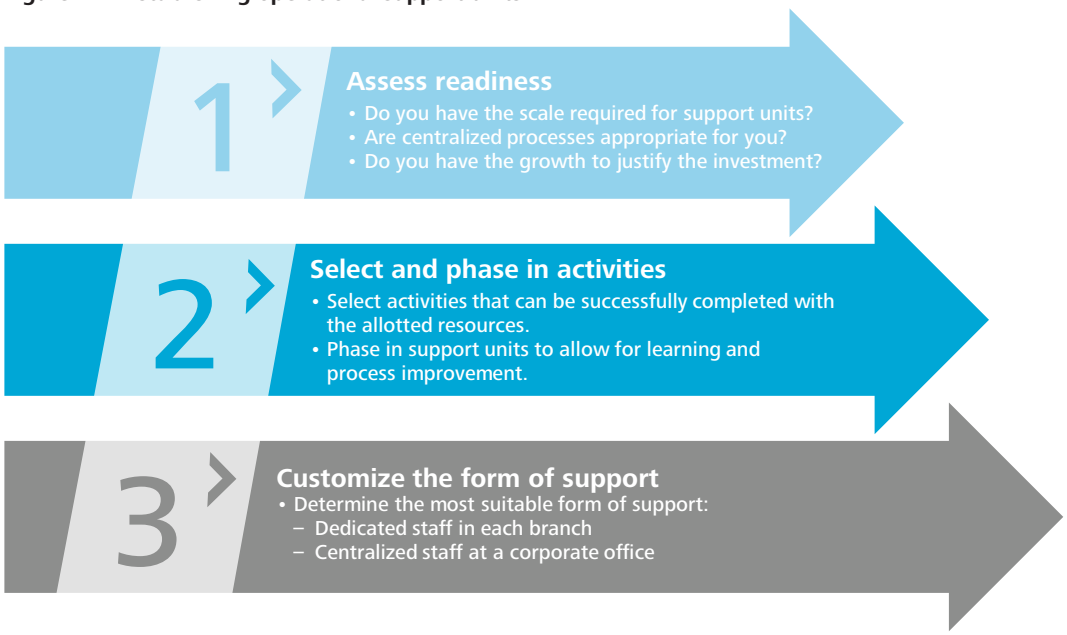
   Suggested action steps: Develop a process for transaction-monitoring results or specialized monitoring rules designed to identify and separate potentially high-risk customers from the moderate- and low-risk customer populations in order to enhance the ongoing risk rating of the customers.

Key considerations

Ongoing operational support of KYC processes is an important part of a robust KYC program. Operations teams should consider the following as they update their processes as part of ongoing KYC improvements:

- Has the end-to-end KYC process been reviewed to identify which steps can be performed by nonclient facing personnel?
- Has cycle time for collection of KYC information as part of onboarding been determined?
- Does the team centralize support units on a regional or country basis?
- Does the team share support units across institutional and retail business?
- Does the team have the scale to create operational support units?

Figure 4 — Establishing operational support units



7 Organizational culture

Importance

Creating a supportive and positive culture of compliance is an important, yet often overlooked, aspect of a mature KYC program. Significant risk-based decisions are made throughout the organization on a daily basis. While compliance programs help govern some of these decisions, fostering the right environment may help continually promote "risk intelligent" behavior, including:

- Understanding the organization's approach to risk
- Taking personal responsibility to manage risk
- Encouraging others to follow proper examples

The challenges surrounding compliance may have increased as institutions sought revenue growth through larger and, potentially in some cases, more global and complex organizations. Yet defining and instilling a risk-aware culture can reinforce major compliance priorities including accountability, information accessibility, information accuracy, information integrity, security, and standardization.

Ensuring the organization values KYC as an important risk management tool, as opposed to a mere compliance requirement, will help build a more effective program.

Common vulnerabilities and suggested actions

Ideally, integrating KYC into the firm's broader internal communication plan — utilizing a variety of channels and methods — can help mold culture. Messages should reach all levels of the organization and highlight both the broad importance of KYC as well as the value of specific KYC processes. Furthermore, assessing staff's sentiment and engagement related to KYC is an important part of managing organizational culture. Finally, ongoing and role-specific training is key to ensuring consistent awareness and application of KYC across the enterprise. Introductory training should be required at onboarding for all relevant roles and more advanced training should be built into each employee's ongoing learning plan.

As noted above, regulators have issued recent guidance related to the importance of a KYC culture throughout the firm, and specific commentary has focused on the following:

1. Employee performance ratings do not always consider metrics related to KYC activities.

   Suggested action steps: As part of improving awareness of the need to comply, firms should include KYC-related metrics. Holding everyone accountable through the performance management process — including goal setting, performance reviews, and peer feedback — helps to ensure a comprehensive and quality-focused KYC program. KYC expectations should be explicitly stated in the code of conduct, employment contracts, and role responsibilities. In addition, managers may wish to include KYC-specific goals in employee year-end success measures. Where appropriate, key performance indicators should assess the fulfillment of KYC processes and be factored into performance incentives, bonuses, and merit increases.

2. Another area involves management communication to employees: the fact that frequent communication regarding the program is informational in nature and sometimes doesn't speak to specific rollout actions that the program has taken can lead to employees questioning the benefit of the program.

   Suggested action steps: Leaders should ensure that KYC-related communications include performance results in order to share valuable progress metrics with employees. While direct-from-the-top communications should be one of the tools used to convey the importance of KYC, cascading specialized messages through middle management and staff can further instill KYC discipline. This approach spreads awareness and instills responsibility for KYC across all levels of management.

Key considerations

Financial institution leadership and talent organizations should examine their employee incentive structures and communications, asking themselves the following questions:

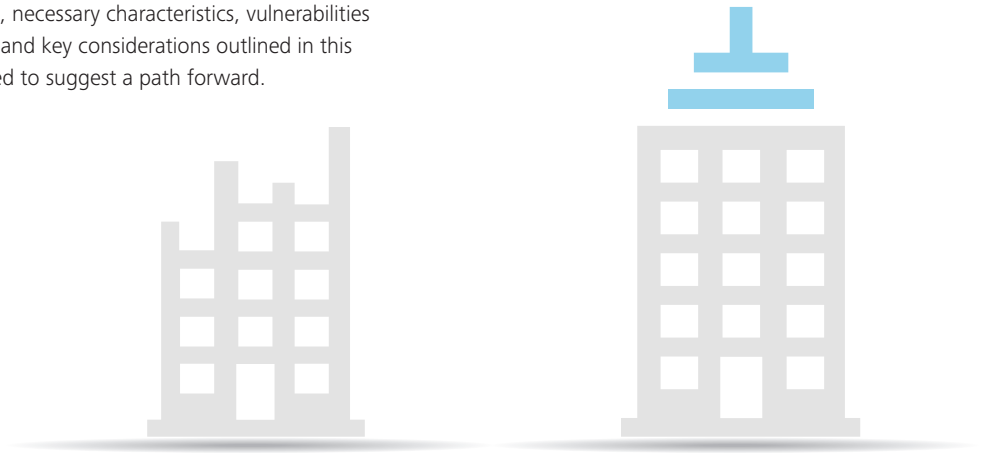
- How do I align incentives with the KYC program?
- What type of communication is most effective for program requirements?
- Do we have comprehensive AML and KYC training for all employees?
- How am I incentivizing compliance for my front-end employees?
- Does my bank do a good enough job at balancing the customer experience and regulatory expectations?

Moving forward in an age of new threats

KYC programs are an essential tool in managing and defending customer financial crimes. For KYC programs to be effective, they must account for new money laundering and financial crimes threats and more advanced technologies.

Given this dynamic, the regulatory pressure to create more mature KYC programs is not expected to recede any time soon. Ensuring against costly regulatory actions, a national security threat, reputational risk, and shareholder lawsuits, financial institutions should allocate the resources necessary to improve their KYC and AML programs.

Optimizing a KYC program can be a complex task, but the seven dimensions, necessary characteristics, vulnerabilities and action steps, and key considerations outlined in this paper are designed to suggest a path forward.



"Based on the enforcement cases I have seen time and time again, both during my time as a prosecutor at the US Department of Justice and now as Director of FinCEN, I can say without a doubt that a strong culture of compliance could have made all the difference."[3]

— Jennifer Shasky Calvery, Director of FinCEN, August 12, 2014

3. Remarks of Jennifer Shasky Calvery, Director of FinCEN, at the 2014 Mid-Atlantic AML Conference, Washington, DC, August 12, 2014, http://www.fincen.gov/news_room/speech/pdf/20140812.pdf.

Contacts

Executive sponsors

Michael Shepard
Principal
Deloitte Transactions and Business Analytics LLP
+1 215 299 5260
mshepard@deloitte.com

Michael Fernandez
Principal
Deloitte Consulting LLP
+1 703 251 3572
micfernandez@deloitte.com

Industry leadership

Kenny M. Smith
Vice Chairman
US Banking & Securities Leader
Deloitte LLP
+ 1 415 783 6148
kesmith@deloitte.com

Deloitte Center for Financial Services

Jim Eckenrode
Executive Director
Deloitte Center for Financial Services
Deloitte Services LP
+1 617 585 4877
jeckenrode@deloitte.com

The industry leadership and Deloitte Center for Financial Services wish to thank the following Deloitte professionals for their insights and contributions to this report:

Christopher Doroszczyk, Principal, Deloitte Consulting LLP
Timothy Partridge, Principal, Deloitte Consulting LLP
Greg Pavlik, Principal, Deloitte Consulting LLP
Clint Stinger, Principal, Deloitte Transactions and Business Analytics LLP
Kakul Sinha, Senior Manager, Deloitte Consulting LLP
Val Srinivas, Senior Manager, Deloitte Services LP
Michelle Chodosh, Marketing Manager, Deloitte Services LP
CJ Chugg, Manager, Deloitte Consulting LLP
Travis Jarae, Manager, Deloitte Transactions and Business Analytics LLP
Mary Katherine Strong, Senior Consultant, Deloitte Consulting LLP

Deloitte Center *for* Financial Services