KPMG

The future of financial crime

Comply. Integrate. Automate.

kpmg.com/us/forensic


KPMG

Introduction

The election of a new U.S. president has brought about a vastly different perspective on financial regulation. However, while regulatory and compliance priorities may shift, the pressures on financial institutions to comply with financial crime regulation will continue. In fact, anti-money laundering (AML) enforcement is expected to remain a key focus of the new administration.

So what does the future of financial crime compliance look like?

This paper sets forth five key areas that compliance officers should consider as they assess and prioritize investments to pave the foundation for their future financial crimes programs.

1. Culture of compliance
2. Integration
3. Data and technology infrastructure
4. Regulatory change management
5. Staffing model and digital labor

Compliance officers will benefit from prioritizing workstreams and evaluating how investments in these areas will impact their organizations' AML and financial crime compliance approach and benefit the institution overall.

Balancing the need to comply with integration and automation

In recent years, regulators have required financial institutions to maintain increasingly robust and integrated AML programs. This has required significant investments of time, money, and resources by AML officers[1] just to meet existing regulatory requirements and expectations. In addition to these regulatory pressures, compliance costs have soared, it has become increasingly difficult to identify and retain qualified AML employees, and liability for AML compliance violations are on the rise.

Compounding these issues, innovators, disruptors, and lackluster economic growth[2] are putting financial strain on firms. As a result, many AML officers have only concentrated on meeting current regulatory expectations to avoid fines—a reactive approach to compliance. The unintended result is that compliance spending is disproportionately allocated to tactical responses and not program enhancements. Such short-term focus has left many AML officers with fewer resources for the strategic thinking, innovation, and prioritization that are needed to develop a sustainable and cost-effective framework for addressing financial crime.

AML compliance is successful when there is integration across an enterprise and successful automation of processes. Going forward, AML and financial crime compliance officers (collectively referred to as "compliance officers") who can manage their compliance programs faster, more cheaply, and more effectively than their peers can realize a competitive advantage for their institutions. This becomes particularly critical in today's economy.

It is a delicate balance to simultaneously anticipate change while continuing to satisfy current expectations. Executive management and compliance officers should focus on where their programs need to be in the next five years—and act now to develop a defined plan for getting there. Marketplace disrupters should not be viewed as roadblocks, but as opportunities to find new ways to solve problems and create value.

When thinking about the future of financial crimes, compliance programs must be strategically designed with input across the three lines of defense—The business, risk management and compliance, and internal audit. There must also be a complete understanding of the institution's inherent risks and risk trends. By dedicating appropriate funds to address both current and future needs, compliance officers can better position their institutions to manage risks and balance operational and business needs. This approach will also enable the compliance officer to thoughtfully design a future financial crimes program that is more dynamic, agile, integrated, digitized, and competitive.

---

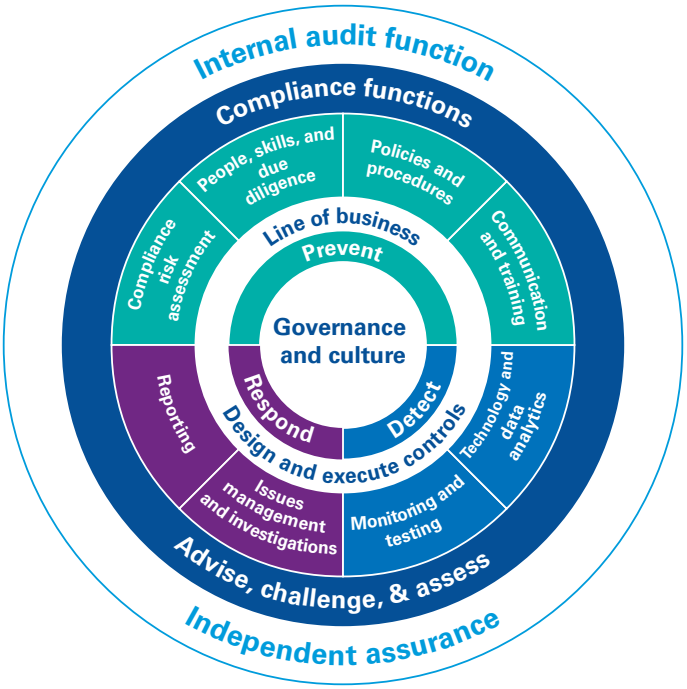
[1] Although this article references AML officers in particular, it is recognized that some larger financial institutions have or may be considering restructuring their compliance programs to create a financial crimes umbrella that would encompass AML, sanctions, frauds, anti-bribery and corruption, surveillance, and other similar compliance matters. These institutions have appointed a Financial Crimes Compliance Officer to oversee and direct this program and they may also find this article valuable.

[2] "U.S. GDP Grew a Disappointing 1.2% in Second Quarter," *The Wall Street Journal*, Morath, Eric and Jeffrey Sparshott, July 29, 2016.

Utilizing a framework for compliance

Financial institutions should strategically invest in initiatives focused on the long term, while concurrently prioritizing immediate program needs and effectiveness. To assist financial institutions in maintaining and refining their compliance programs, KPMG has developed a proprietary Financial Crimes Program framework that consists of eight components, with governance and culture at its core.[3]

As financial institutions advance in their financial crimes compliance journey, their compliance activities shift from responding and remediating to proactive prevention and detection. This allows for greater efficiency, sustainability, and agility. And also helps institutions to think about compliance not just as a cost of doing business, but as a competitive advantage.



Comply

Comply with current regulatory requirements and expectations. Objectives include tracking of issues; remediation of gaps; inventory of existing financial crimes regulatory obligations; designing and implementing enhanced financial crimes compliance policies, procedures, processes, and controls to comply in their existing regulatory landscape; and preparing for future regulatory requirements.

Integrate

Further integrate the financial crimes program enterprise-wide. As financial institutions mature in their compliance approaches, they typically seek to break down organizational silos in favor of a more centralized approach. This change impacts their governance structure, reporting, monitoring, testing, risk assessments, investigations, screening, technology, and data needs.

Automate

Further automate the financial crimes compliance activities for even greater consistency, efficiencies, and agility. At this stage, financial institutions seek to further automate rule scanning, negative news, sanctions scanning, due diligence, monitoring and testing, risk assessment processes, surveillance, investigations, work flows, reporting including development of dashboards, and data governance.

Current → **Future**

[3] The KPMG framework integrates the U.S. Federal Sentencing Guidelines suggestions for compliance programs as a foundation and goes beyond those concepts to incorporate regulatory AML, Sanctions and Anti-Bribery and Corruption (ABC) requirements, guidance, and leading initiatives by peers.

1 Culture of compliance

The presence of a strong compliance culture establishes the foundation for, adherence to, and responsibility for regulatory requirements within everyday practices. When a financial institution does not have the right culture or a fundamental commitment to "doing the right thing," the institution is vulnerable to misconduct, specifically financial crimes misconduct (i.e., AML, fraud, etc.). Failure to instill a culture of compliance can carry significant costs, including fines, reputational harm, and damage to the business.

Regulators are increasingly focusing on the culture of compliance, including AML culture, at the institutions they examine. This includes looking at:

- Management's commitment to, and support of, a culture of integrity and compliance throughout the institution
- How compliance leaders regularly assess culture
- How incentives and disciplinary protocols are aligned with the desired culture (such as promotions, pay incentives, etc.)
- Whether there are any subcultures that impair an institution's cultural values
- Whether senior leadership, including management within the business units, consistently reinforces the message of compliance by setting the tone from the top. When compliance can be overridden by the business, and improper conduct exists without accountability, the compliance function may be rendered ineffective[4]
- How the board evaluates root causes of misconduct and whether they timely mitigate systemic issues
- The key risk indicators (KRIs) and metrics information that the board of directors and executive leadership receive, indicative of an institution's cultural "health"
- How willing employees are to escalate and raise issues when they observe inappropriate behavior and whether effective challenge exists.

This notion that a strong culture of compliance is critical,[5] specifically AML compliance[6] is demonstrated through guidance and enforcement actions. The Financial Crimes Enforcement Network (FinCEN), for example, has recently identified culture of compliance as a factor in regulatory exams and violations, In 2014, FinCEN issued an advisory on culture, highlighting the importance of a strong culture of AML compliance for senior management, leadership, and owners of all financial institutions.

[4] In October 2016, The Monetary Authority of Singapore fined three (3) banks and revoked the licenses of two (2) of these institutions; also see Thompson Reuters, "Lessons from BSI and Falcon Private Bank: Compliance Needs Authority to Play Effective Role," Patricia Lee, October 20, 2016.

[5] The Financial Industry Regulatory Authority (FINRA) defines "firm culture" as "the set of explicit and implicit norms, practices, and expected behaviors that influence how employees make and carry out decisions in the course of conducting the firm's business." See FINRA's 2016 Regulatory and Examination Priorities Letter dated January 5, 2016.

[6] FinCEN Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance, FIN-2014-A007, August 11, 2014.

Globally, regulators are identifying poor culture as the root cause of many types of misconduct. To be prepared, compliance leadership, in conjunction with executive management and often the board of directors, should be able to demonstrate that steps have been taken to assess their culture of financial crimes compliance, possibly as part of a larger compliance effort, and that they have identified and properly scoped any cultural issues, as well as the root causes of such issues, and responded timely to instances where it seems the culture of compliance may not be a focus or as strong. The institution must also be able to demonstrate a strong commitment at the top, as well as in the middle, with a focus on capturing and understanding systemic risks and mitigation of those risks, including making hard decisions like termination of high sales performers.

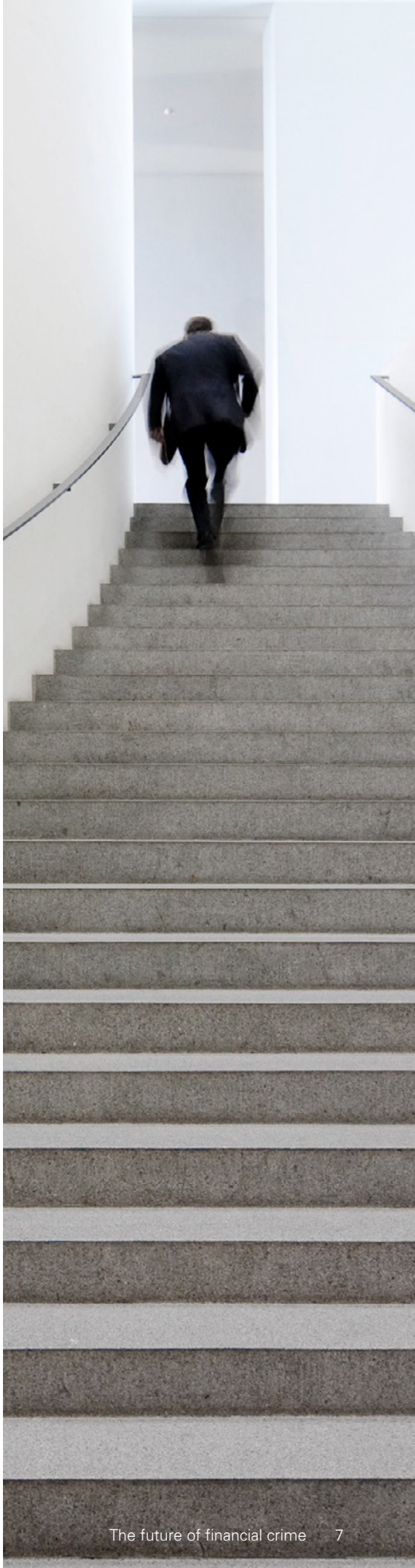
An investment in a strong compliance culture is an investment in prevention, which is the most fundamental control an institution can put in place to reduce misconduct.

FinCEN's advisory to U.S. financial institutions on promoting a culture of compliance

As set forth by FinCEN, a financial institution can strengthen its AML compliance culture by ensuring that:

- Leadership is supportive
- AML efforts are not compromised by revenue interests
- Information is shared between departments throughout the organization
- Resources are sufficiently allocated
- AML program undergoes independent testing
- Leadership and staff understand AML efforts and reporting.[7]

[7] FinCEN Advisory to U.S. Financial institutions on Promoting a Culture of Compliance, FIN-2014-A007, August 11, 2014.



2 Integration

Rogue employees. The use of shell companies to perpetrate frauds. Insider trading. Bribery and corruption. Financial crimes such as these have historically been addressed in silos, limiting an institution's ability to holistically evaluate the issues, respond, and remediate. It can also result in duplication of efforts, which can be very costly. Institutions should strongly consider integrating their AML program under a formalized financial crimes compliance structure.

Regulators agree. They are increasingly expecting a consistent approach to financial crimes compliance across organizations. This can be very complicated for an organization that has siloed compliance efforts. In the immediate term, organizations can begin by creating better coordination and communication mechanisms between their various compliance units. However, segregation of teams, tailored training for different functions, and limitations in the data available to each compliance unit remain significant obstacles to a concerted financial crimes approach.

To create more effective and efficient compliance across the financial crimes spectrum, organizations should break down business unit barriers by fully integrating teams, systems, and processes under one financial crimes umbrella. By combining budgets and resources, greater operating efficiencies and cost savings can be achieved. A financial crimes structure also improves information sharing, reduces redundancy, and allows for greater collaboration and a more refined strategic vision.

In addition to further integrating the compliance function, organizations can also benefit from breaking down business unit silos and individualized approaches to managing financial crimes risks. This will strengthen the institution's ability to understand and manage its financial crimes risks centrally and to analyze, size, and escalate issues when warranted. This can be accomplished by establishing enterprise-wide monitoring and testing protocols that the business units will utilize, procedural standards, communications, and risk assessment templates and methodologies.

3 Data and technology infrastructure

For financial institutions to meet their regulatory and compliance obligations, they must understand how technology is used across departments and business lines, integrate technology where possible, or at minimum have a dashboard that aggregates data across disparate systems. In today's environment, financial institutions tend to have disjointed technology systems that support their AML, fraud, and other financial crime compliance activities. This non centralized structure also applies to core systems that collect and maintain data relevant for AML compliance purposes.

Financial crimes regulatory obligations require institutions to:

- Assess their technology infrastructure, including identifying gaps
- Assess whether data has the integrity and accuracy needed
- Leverage dynamic, multidimensional predictive analytics
- Ensure that systems can adeptly handle regulatory change that is highly probable to occur.

This last item is particularly important. In the last year, significant regulatory expectations have been codified, and further changes are expected. Two newly promulgated regulations that will require investment in technology infrastructure are a risk-based banking rule Rule 504—implemented by the New York Department of Financial Services (DFS)—and the new customer due diligence (CDD Rule)[8] codified by FinCEN.[9]

Rule 504 requires financial institutions with operations in New York to implement a transaction monitoring program and watchlist filtering program, with specific requirements outlined for each. These include validation of the systems the institution utilizes (data feeds in and out) and assurance of data integrity, accuracy, and quality standards.[10] While the compliance function is a user and consumer of data, it is not considered an "owner" of data. However, Rule 504 requires systems testing and validation, demonstrates that there is an expectation that compliance understands its data, tests it, and confirms that technology infrastructures and data do not have gaps that impact program effectiveness.

[8] The FinCEN Rule, effective July 11, 2016, outlines customer due diligence requirements not previously explicit in the Bank Secrecy Act, and also includes new requirements to identify and verify the identity of beneficial owners of legal entity customers. Final Rule, Customer Due Diligence Requirements for Financial Institutions.

[9] FinCEN is a primary U.S. administrator and regulator of BSA/AML regulation.

[10] The DFS Rule requires financial institutions, in part, to establish processes for "identification of all data sources that contain relevant data," "validation of the integrity, accuracy and quality of data to ensure … accurate and complete data flows through the Transaction Monitoring and Filtering Program," and that "Data extraction and loading processes [enable] a complete and accurate transfer of data from ….source(s) to automated monitoring and filtering systems, if automated systems are used."Final Rule, Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications. For further information, see DFS June 2016 Press Release.

The CDD Rule codifies CDD requirements that, for many institutions, will require enhancements to their KYC process, procedures, and technology infrastructure by May 11, 2018. While the CDD Rule permits CIP (Customer identification program) reliance to extend to CDD requirements and does not establish standards be retroactively applied, most institutions anticipate a significant impact from this regulatory change. In particularly, many will need to:

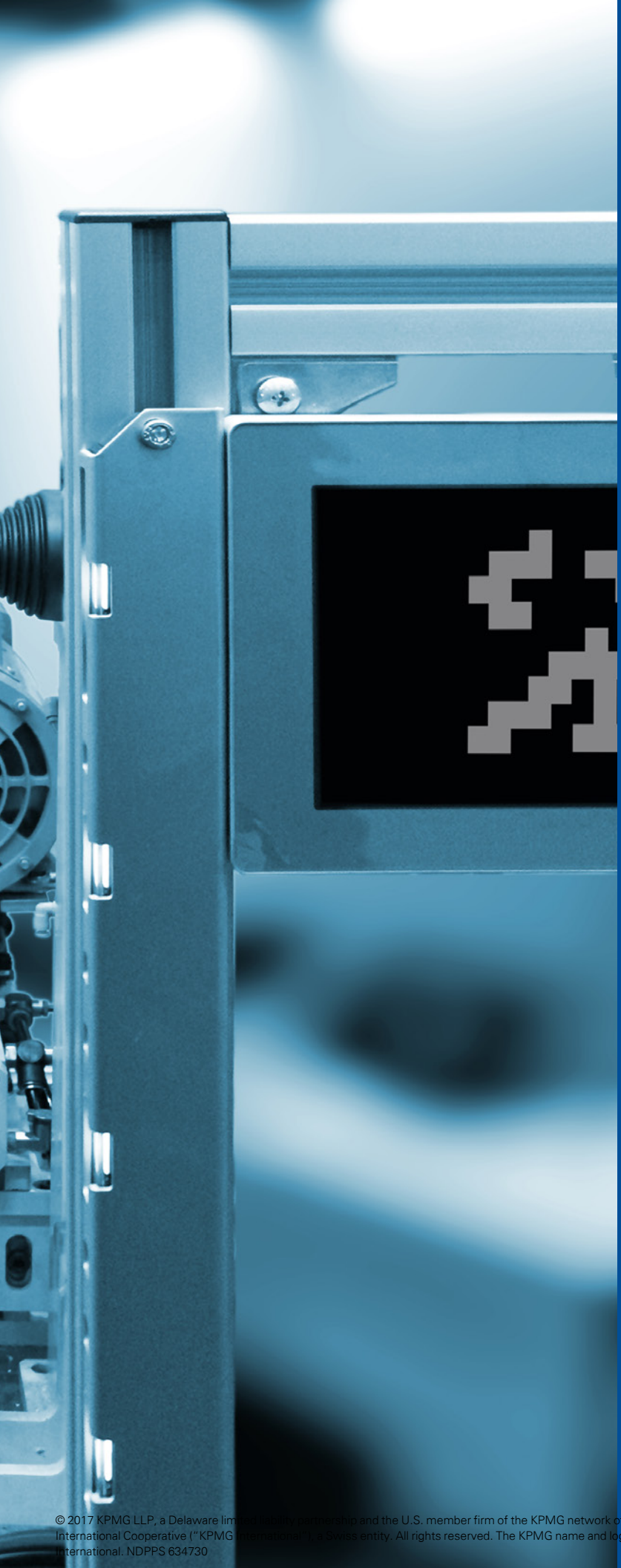
- Develop customer risk profiles
- Identify and verify Beneficial Ownership and Controlling Parties
- Risk-based updating of customer information and greater integration of KYC (Know your customer)/CDD with monitoring and reporting efforts
- Certification Requirements
- Identification and implementation of new key risk indicators (KRIs) to capture risks identified in the above areas.[11]

To satisfy these newly issued regulatory and reporting requirements, as well as other regulations on the horizon, financial institutions need to not only continuously invest in their technologies, but anticipate future regulation to better assess synergies across the institution with existing controls. Such investments must always be driven by a strategic vision of where AML and financial crime regulation is headed and what the future regulatory regime will require. Firms should seek out new and innovative technologies that can achieve greater efficiencies while improving the internal control environment. Tactical investments in the area of technology should have long-term benefits for both compliance and the profitability of the business.

Investing in technology without a partnership with operations and a clear and grounded strategy from the C-suite can derail the journey and waste much-needed dollars. Business strategy must be an instrumental consideration in the design and implementation of an AML risk mitigation strategy, which can then be embedded and supported by technology infrastructure.

[11] FinCEN acknowledges that certain aspects of the CDD rule, like the identification or verification of beneficial owners and the housing and maintenance of this data, will require significant technological and operational changes, which are thereby likely to result in increased costs. For further information, see the Regulatory Impact Assessment.


Temp Min
15,56 C
Temp Max
33,94 C
Temp Ambient
32,13 C
Date
XX-XX-XXXX
Time
XX:XX
Job
WW25D76
Customer
Status
Scale
MAX



To comply with the CDD Rule and Rule 504, institutions are increasingly looking to enhance their technology and data analytics to achieve a strategic and risk-based approach to new requirements. For example, technology solutions can assist KYC teams in collecting ultimate beneficial ownership (UBO) and controlling party/directors information to meet the CDD Rule requirements, from public sources as well as subscription sources. In addition, technology can support the institution in maintaining a customer risk profile and ongoing screening as part of this process. Importantly, technology can also be embedded to further link the institution's KYC databases and transaction monitoring databases, enabling a data used feed that is circular between the two, for a more integrated approach to customer risk.

Furthermore, cognitive technology and data analytics can greatly aid an Institution in identifying patterns of behavior that presents a higher indicia of risk for further investigation. In this way, technology supports a more risk-based approach to transaction monitoring and a tighter vision of customer risk.

4 Regulatory change management

Critical to sustainable compliance is a robust regulatory change management process. This allows the institution to more systematically manage current regulatory risks and anticipate the future. By identifying regulatory changes on the horizon, a regulatory change management program enables compliance officers to:

- Assess which regulatory changes appear most probable
- Prioritize anticipated changes by the projected impact (i.e., on technology, people, and process)
- Evaluate where convergences occur globally
- Develop a more strategic vision for compliance programs, especially AML.

The need to monitor current and future regulations, both locally and globally, has caused institutions historically to delegate the task of inventorying financial crimes regulations to regional teams within legal or the business units. Such a decentralized approach encourages multiple methods and inconsistent processes for managing regulatory change across an organization.

As regulations continue to converge globally, the need to manage change with consistency at the corporate level becomes essential. A centralized regulatory management program enables a firm to adapt to changes more quickly and efficiently. It also allows for a smooth transition and continued compliance with all applicable laws. Such an exercise should ideally incorporate a corporate methodology for inventorying the regulations and leveraging existing work already completed; a translation of each regulation into "plain English"; and a way to map each regulation to the internal controls, policies, procedures, and processes in place. It should also provide for consultation of legal opinions when regulations are subjective.

Institutions that are currently evaluating their regulatory change management approach should consider the following:

- How does the institution currently track and manage new or updated laws andregulations, regulatory expectations, and guidance?
- Does the compliance officer have sufficient knowledge of the relevant regulatory requirements applicable across all jurisdictions, business units, and products of the enterprise?
- Does the institution track enforcement actions against other financial institutions to identify trends in interpretation and enforcement of existing regulations?
- What is the institution's process for assessing the impact of a regulatory change on its business (e.g. products and services) and internal controls to identify necessary changes?
- How does the institution currently monitor and test its regulatory change management processes?

Once an institution has developed a strategy for regulatory change management with clearly articulated goals, use of technology can provide a sustainable, consistent, and auditable process. An automated technology solution further enables the compliance officer to stay abreast of regulatory changes. It can provide a snapshot of the enterprise-wide impact of a regulatory change and allow the institution to respond with agility.

Regulatory Technology (RegTech) solutions assist firms in moving away from the concept of big data towards one of "smart data." Smart data uses machine learning and intelligent algorithms to make sense of big data's overwhelming volume and complex patterns by structuring these patterns in a cost-effective way that is better able to identify current and emerging risks, predict compliance failures, and enhance business line coordination.

Eighty-four percent of CEOs are concerned about the quality of the data they base their decisions on.

(Source: KPMG International's 2016 Global CEO Outlook Study)

5 Staffing model and digital labor

Over the past few years, institutions have struggled with high attrition rates, particularly within their AML compliance departments, resulting in the loss of institutional knowledge. As salaries have risen, AML compliance employees have rotated in and out of financial institutions in what can often seem like a revolving door. Automated processes and incorporation of digital labor would greatly help AML and future financial crime compliance departments with this human resources issue.

A recent survey distributed by BAE Systems with respect to operational risk reveals a growing preference to solve low-value, redundant tasks like Know Your Customer (KYC) information collection and sanctions screening by using third-party external sources.[12] Compliance officers are encouraged to take strategically assess their staffing needs and how they can augment human labor with automated solutions to keep costs down and increase efficiency and accuracy of core financial crime compliance functions.

A broad staffing assessment should include a strategic plan to invest in key compliance leadership roles and bring well-qualified individuals to their institutions. Most importantly, financial institutions must identify where digital labor and technology advances can be incorporated into the institution's approach to dealing with financial crime.

Recent technological advances present a significant opportunity for compliance officers to use technology to automate various compliance activities and improve customer experience. Digital labor[13] can be used, at minimum, for traditional labor-intensive processes. It can also augment or automate tasks currently undertaken human workers.[14] At its most advanced level, digital labor[15] incorporates technology and predictive elements that can help digitize KYC, transaction monitoring and compliance function surveillance, and testing processes. This ultimately creates cognitive abilities within a regulatory automation structure.[16]

[12] See the 2016 Financial Crimes Survey, published by BAE Systems and Operational Risk. The BAE Survey Report indicates respondents prefer in-house solutions for KYC/CDD (40.3% of respondents) and AML transaction monitoring (26.4% of respondents) with additional respondents utilizing a combination of internal and external solutions.

[13] Also termed "automation of labor" or "Reg Tech"

[14] See KPMG's "Demystifying Digital Labor," 2016, available at http://www.kpmg-institutes.com/content/dam/kpmg/advisory-institute/pdf/2016/demistifying-digital-labor.pdf.

[15] See KPMG's "Monitoring and Testing: Enhancing your compliance effectiveness and agility," 2016, available at https://advisory.kpmg.us/content/dam/kpmg-advisory/risk-consulting/pdfs/2016/compliance-testing-monitoring-web.pdf.

[16] Demystifying Digital Labor.

"Digital labor and cognitive learning present opportunities for financial institutions to become more effective and efficient in managing their financial crime risks and therefore, more strategic in their compliance activities. The investment can vary in cost from relatively small for Robotics Process Automation, RPA, to significant for cognitive learning. Financial institutions will need to weigh the costs and benefits related to any activities in this area. However, the question is not if digital labor and cognitive learning are the future but rather how quickly the future becomes now. Those institutions that embark on a reasoned strategic journey in this space will undoubtedly find significant value and competitive advantages."

– **Stephen D. Marshall**
Principal, Advisory

One type of cognitive technology system, known as machine learning, can be applied to identify overall trends or patterns in disparate data. The results or pattern can then be used in live circumstances and/or to further assess risks in a broader population of data that may contain similar trends. It can even be used to make predictions by comparing existing information to new data. Predictions improve as more data is reviewed. From a cost/benefit perspective, it is estimated that up to 45 percent of workplace activities can be automated. As a result, the benefits of digital labor typically include higher efficiency and significant cost savings.[17]

Understanding the phases of digital labor

Digital labor can be used to varying degrees depending upon the investment an institution is prepared to make and the returns the institution wants to realize. Here are some options and context for incorporating digital labor into financial crimes compliance programs:

Robotic Process Automation

Institutions seeking the most basic form of digital labor begin with Robotic Process Automation (RPA), which leverages known rudimentary processes found in many organizations today. Machines follow specific steps in these processes just as a human would be asked to. RPA may be applied to basic financial crime functions, such as account closings, transaction processing, process mapping, and other easily repeatable tasks. These types of RPA capabilities are already prevalent among AML programs, which are looking to advance along the digital labor continuum.

Enhanced process automation

As an institution goes further in utilizing and integrating digital labor, they can begin to explore enhanced process automation (EPA). This includes all of the aspects of RPA as well as additional functionalities to enable capabilities to process complex structured data. EPA tools can process a high number of complex transactions and require a deeper level of analytics.[18] As it pertains to financial crime, institutions can use EPA to implement built-in knowledge repositories that enable structured data ingestion to enhance their regulatory change management approach. EPA can also be leveraged for repeated manual activity subject to validation and structured questions and responses—facets of testing and monitoring that can become more streamlined with EPA.

EPA can help automate aspects of the transaction monitoring process (such as negative news screening and assessment of red flag activities) as well as suspicious activity reporting. For this reason, EPA is often utilized for KYC processes to collect information digitally up front and to look across an institution for shared customers in order to limit requests and outreach to customers when they purchase a new product and/or service.

[17] Id.

[18] Id.

KPMG

Cognitive automation

The most mature level of digital labor is cognitive automation (CA), which comes into play when "cognitive software mimics human activities such as perceiving, inferring, gathering evidence, hypothesizing, and reasoning."[19] Unlike humans, CA has the ability to retain and analyze considerable amounts of unstructured data. When cognitive software is automated, digital labor is capable of "judgment-intensive tasks," including the ability to "read and extract meaningful information out of unstructured data," which accounts for approximately 80 percent of the world's data.[20] CA software can revolutionize the KYC process, since much of KYC information can be obtained as highly unstructured data inputs from various sources. CA can enable automatic transference of this information into an institution's technology system and populate fields with requisite data points. This most advanced stage of digital labor will also enhance surveillance and monitoring with unstructured variable changes,[21] as well as automate aspects of regulatory change management.[22] The implementation of CA is just beginning and will require a significant investment in time and resources before reaching its full potential.

Closing thoughts

As regulatory pressures continue to mount and new entrants render the marketplace more competitive, financial institutions need to be agile. A reactive response to compliance requirements is not the way of the future, as it can be costly and ineffective. To maintain a competitive advantage, financial crimes officers need to pursue strategic compliance investments. By refining their AML programs or shifting to a financial crimes approach, and further investing in the five key areas—culture of compliance, integration, data and technology infrastructure, regulatory change management, staffing model and digital labor—AML and financial crimes officers can help to position their programs to compete in the future.

[19] Id.

[20] Monitoring and Testing: Enhancing your compliance effectiveness and agility.

[21] Id.

[22] Id.

Contact us

Teresa Pesce
Global AML and Financial Crimes and Enforcement Leader
T: 212-872-6272
E: tpesce@kpmg.com

Authored by Michelle Harman, Grace Barclay, and Nicole Stryker, with contributions from Jordan Seiferas.

Some of the services described herein may not be permissable for KPMG audit clients and their affiliates.

kpmg.com/socialmedia