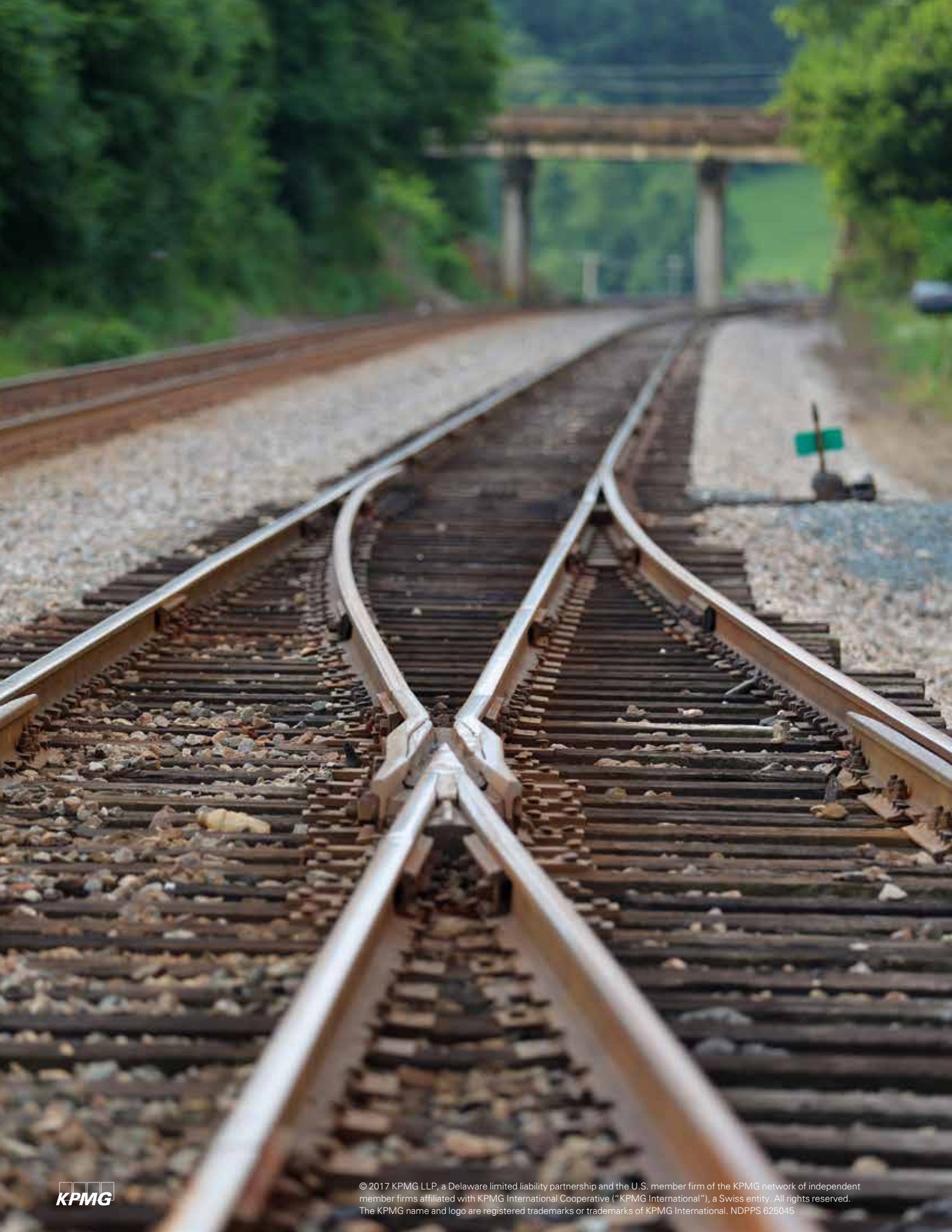
KPMG

Under one agile umbrella

An approach to managing financial crimes risk

kpmg.com/us/forensic



More than ever before, financial institutions are challenged to meet financial crimes compliance obligations in a more cost-effective and agile way. As the economic environment promises continued uncertainty and increased competition—including from emerging and innovative FinTech firms—institutions must become more strategic and intentional in how they manage risk. Many financial institutions, are addressing this by integrating their existing anti-money laundering (AML), sanctions, fraud, surveillance and anti-bribery and corruption (ABC) compliance programs under a unified financial crimes umbrella. However this journey, once undertaken, must be well-designed and carefully managed.

Increasingly, financial institutions are viewing their financial crimes risks in the aggregate and under one umbrella. What transformative value does an integrated financial crimes program provide to your institution?

The pressure to be more agile and dynamic

Over the past few years, financial institutions have been confronted with a host of financial crimes risks and scandals ranging from manipulations of LIBOR rates to rogue trading, money laundering, sanctions, cybercrimes, human trafficking, fraud, bribery and corruption, and market manipulations (to name a few).

Regulators increasingly expect Chief Compliance Officers (CCOs) to achieve greater consistency in their approach to managing diverse financial crimes risks across the enterprise; establish greater coordination and collaboration; achieve more robust information sharing; further integrate technology enabling an enterprise-wide view of their risks; and consider how predictive data analytics can be used to enhance their risk-based monitoring.

In addition to these regulatory pressures, many financial institutions are being challenged by new entrants to the marketplace in addition to their traditional competitors, all while operating in a lower profit margin environment. This is compelling some institutions to assess whether their approach to financial crimes risk can be more agile and dynamic, even as they further cut costs to realize greater compliance value and competitive innovation.[1]

This publication will discuss in more detail some of the regulatory drivers that are encouraging CCOs to integrate their approach to managing financial crimes risk; the governance benefits of further structural integration; and a road map for considering how to execute and embark on this journey.

[1] See "The Compliance Investment: Realizing the value of compliance through greater effectiveness, efficiency and sustainability" https://advisory.kpmg.us/content/kpmg-advisory/risk-consulting/compliance-transformation/compliance-investment.html.

Industry trend: Implementing a financial crimes approach to managing risk

Many financial institutions[2] are reevaluating their approach to how they manage financial crimes risk, and are creating a common governance strategy and umbrella structure to better manage compliance.

To create such a structure, CCOs in conjunction with their AML and Sanctions Officers as well as other key stakeholders should:

1. Establish a strategic vision of their future financial crimes program, engaging and collaborating with senior management in the first line of defense (lines of business and operations) in its design and obtain buy-in from the board of directors
2. Integrate teams that are siloed and separately dedicated to the compliance of distinct regulations such as AML, sanctions (including Office of Foreign Asset Controls (OFAC)) compliance, fraud, or ABC compliance, among others
3. Update or enhance the institution's technology infrastructure
4. Designate an individual with expertise and authority, to serve as the institution's Financial Crimes Compliance Officer.

Institutions that are evaluating whether they should integrate their financial crimes compliance efforts may look to the experiences of peers to serve as a roadmap for their journey, and provide insights into the costs and benefits that may be realized. Based upon this, executive leaders can consider if a shift in their financial crimes risk management approach makes sense given their business model and goals.

In addition, this exercise can further a CCO's understanding of the institution's existing compliance programs for each financial crimes risk. For example, by virtue of being a cross-regulation exercise, the assessment may shed light on gaps or differences in approach or the best practices of one team that can be shared and adopted by others.

It can also paint a more robust and holistic picture of the financial crimes risks by exposing the internal controls and processes across the institution that would normally only be visible in isolation in the institution's ABC or AML risk assessments, or that might be buried in a higher-level compliance or Governance Risk Compliance (GRC) risk assessment.

As an additional incremental benefit, this exercise creates an opportunity for the CCO (and the compliance function) to engage in dialogue with stakeholders and senior leaders across business units, operations, and technology, thereby raising the profile of the CCO and the vision of compliance as a "partner" with the business lines in key strategic decisions.

Based upon this exercise, some CCOs may find a phased approach makes the most sense.

How did we get here?

Historically, financial institutions have tended to manage each of their financial crimes risks largely in siloes, implementing a level of communication, coordination, and joint reporting only to meet their regulatory obligations.

Since a financial institution's obligations for each of these risk areas can be nuanced and the regulatory requirements/sources differ, it is understandable why many institutions continue to retain this historical, siloed approach, particularly since, in the past, institutions have been able to meet the expectations of their various regulators while maintaining their legacy structures and infrastructure.

[2] The 2016 Financial Crimes Survey, published by *BAE Systems and Operational Risk,* reports that in 2016, 76.6% of financial institution respondents indicated they use consolidated fraud and compliance solutions compared to 65.7% in 2013, (a 10 point jump) suggesting that financial institutions can benefit from combining their fraud and AML resources to create efficiencies and identify crossovers.

KPMG

Regulatory trends: Driving change

Globally, regulations impacting an institution's approach to managing financial crime risk are converging. For example, a U.K. law requiring compliance certifications became effective in 2016, and more recently the Department of Financial Services (DFS) in New York implemented AML regulations that require compliance certifications. These laws collectively reflect an intensified focus by global regulators on ensuring that compliance leaders within financial institutions are accountable for their compliance program (and potential deficiencies).

— **Senior Managers and Certification Regime (SM&R)** – On March 7, 2016, the United Kingdom's SM&CR[3] law, applicable to specific types of financial institutions, became effective.[4] The rule requires that covered financial institutions designate a "senior manager" of stated seniority to render an annual certification that the institution is managing its financial crimes risks. This means that one individual must oversee management of financial crimes compliance defined to include fraud. Thus one supervisor is responsible and accountable for the actions of their subordinates.

— **New York Regulation** – On June 30, 2016, the DFS, which regulates New York State-chartered banks, published an AML regulation effective as of January 1, 2017 requiring banks, as of April 15, 2018, to submit annually a board resolution or a finding from a senior compliance officer confirming the institution is in compliance with the regulation.[5]

Also, in recent months, the Panama Papers have sparked many countries, including the United States, to implement new customer due diligence requirements and laws aimed at addressing financial crimes risks posed by shell companies.

Since shell companies can be used in a range of financial crimes, from money laundering, sanctions violations, and fraud to human trafficking, an integrated cross-regulation approach to managing the risks of these clients, and internal coordination during investigations, is even more important.

To this point, notable internal investigations within financial institutions this past year have also showcased the interconnectivity of many financial crimes and the need for a more integrated, consistent approach, particularly in due diligence and transaction monitoring.[6]

[3] The reforms to the regulation of senior bankers are contained in the Financial Services (Banking Reform) Act 2013 Part 4. They derive from the Parliamentary Commission on Banking Standard recommendations in June 2013.

[4] The law specifically includes, but is not limited to, banks, building societies, credit unions, and certain large investment firms established in the United Kingdom, including U.K. subsidiaries of overseas firms. Further expansion of the regulations are expected through 2018.

[5] See "New York Banking Regulator to Publish New Rules to Fight Money Laundering" by the *Wall Street Journal* Web site, June 29, 2016, Christopher M. Matthews

[6] See "1MDB: The Inside Story of the World's Biggest Financial Scandal" by the Guardian Web site, July 28, 2016, by Randeep Ramesh

Added benefits and value: An approach to managing financial crimes risk

Generally, designing and implementing an integrated financial crimes program under an umbrella structure presents many benefits for a financial institution. These include:

- Improved integration, coordination, and collaboration to manage financial crimes risk across the institution (including with the first line of defense)
- Improved data aggregation and data analytics and an enhanced technology infrastructure through investment and realignment of data feeds into a common repository
- Expanded view of financial crimes risks and trends for the board of directors and senior management (predictive measures)
- Heightened board of director awareness and understanding of risks and strengthened control environment
- Added cost savings resulting from reductions in complexity and duplication
- Enhanced ability to comply with changes to the institution's regulatory expectations.

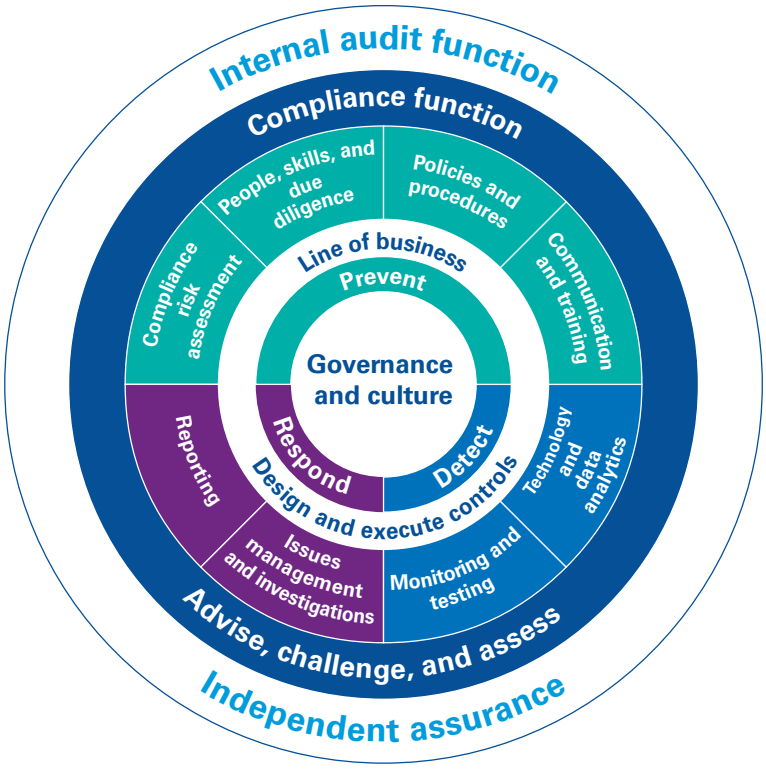
KPMG

Our Financial Crimes Compliance Framework

When establishing or enhancing an institution's financial crimes program, compliance leaders are embarking on a journey that will impact their people, processes, and technology across all three lines of defense.

As with other types of compliance journeys, there is not a "one size fits all" approach. Where one institution may be able to transform its program into a targeted state quickly, others may need to implement a phased approach. Regardless of the approach, the journey must always be deliberate, intentional, and strategic.

KPMG's proprietary Financial Crimes Program Framework



Since program components are interconnected, institutions cannot make changes in isolation to one program component without considering if the change has unintentionally created a gap and/or weakness elsewhere in the program.

To illustrate, consider that to establish a financial crimes program, at the core, an institution will need to redesign a large swath of its compliance structure, integrating it under one new compliance leader and one "umbrella." This is depicted in the Financial Crimes Framework as "Governance," with many other program components needing adjustment to align to and support the change.

For example, in designing a new centralized financial crimes compliance unit, employee roles, and responsibilities will likely shift. Financial crimes policies and procedures may need to be consolidated or rebranded and enhanced to reflect a more coordinated approach and potentially to include new or revised processes. Coordination and escalation/reporting mechanisms may need to be adjusted, and data and technology infrastructure may need to be updated. Changes and/or updates might also be needed in the following areas:

— Onboarding and monitoring of customer activity and related reporting

— Compliance testing program and internal audit program

— Resource reallocation and staffing models

— Training and communications

The journey: A roadmap to a Financial Crimes Program

The journey to an integrated financial crimes program begins with an understanding (and assessment) of the institution's current state, which can be utilized to design a future-state program that is realistic and achievable. The below steps and considerations can help to guide compliance leaders who are considering embarking on this journey.

— Step 1: Consider commencing the journey: Is it valuable to your institution?

Compliance leaders recognize the importance of cultivating partnerships with business leaders and internal audit teams as part of everyday compliance initiatives. This journey towards an integrated financial crimes program is no different. In fact, such relationships are critical for such a substantive and involved effort. Therefore, the first step in the journey to an integrated financial crimes program should be to convene a cross-functional working group that is empowered to assess whether the journey ought to be undertaken based upon perceived benefits, anticipated costs, and a knowledge of the internal workings of the institution, including potential pitfalls and obstacles.

By establishing a cross-functional working group, inclusive of stakeholders across the three lines of defense, collaboration can occur from day one. Compliance leaders can better meet the expectations and concerns of stakeholders in the ensuing months (and even years) and incorporate such information into a realistic project plan that is more likely to resonate with, and obtain buy-in from, all parties, increasing the likelihood of a successful outcome.

All too often, key stakeholders are involved late in the process and lack the ownership to shape the initiative and direction of the journey. This can cause resentment and ultimately derail even the best intentions and ideas, with significant cost to the institution. Alternatively, the wrong stakeholders may be involved—including stakeholders offering little or no insight into the institution's risks, controls, or strategic business direction, or stakeholders without sufficient authority and seniority in their business line to help shepherd the requisite change. This is no less significant of a risk, as it too can lead to failure and lack of adoption/commitment by the institution.

Quite possibly the working group will not have sufficient information at this stage to unequivocally decide whether to give the journey a "green light." Further quantifiable information supporting the benefits of the journey may be needed, which requires additional information as provided for in Step 2.

At this initial stage, however, the goal is to begin a dialogue. Seek input from executive leadership in terms of what supporting information would be necessary for them to consider approving the initiative, understand the value they could expect to realize, and understand the viewpoints of other stakeholders in the first and third lines of defense.

Should the institution decide not to move forward, compliance leaders should aim to understand the decision rationale and to perhaps even document the analysis that occurred.

If compliance leaders feel the journey truly must be undertaken to manage risk, they can, and should, continue to work with their executive leaders to migrate towards the necessary goal.

Tips: Strategically consider the stakeholders who will be part of the working group evaluating the journey benefits and value. Create protocols for the working group that formalize the communication that will occur and will encourage open lines of communication and dialogue so that all members feel comfortable sharing their perspectives. Develop a work plan to document the scope and breadth of the goals and the necessary steps to achieve those goals, as well as to keep all stakeholders and executive leadership aligned throughout each of those steps.

— Step 2: Understand the current state

When embarking on this journey, compliance leaders will want to ensure they have appropriately sized their approach and target state to address current and anticipated risks, including those related to changes to their business/operations. This can only be accomplished if the compliance leader has a clear vision of its underlying inherent financial crimes risks and the institution's existing risk management controls and processes to mitigate the risks.

Too many institutions fail in this respect by adopting models that may have worked for larger or more regulated institutions or conversely for smaller institutions with a different product mix or jurisdictional presence. External subject matter experts can provide valuable benchmarking insights and best practices, as well as share common pitfalls that have resulted in missteps for other institutions. These individuals, however, cannot and do not replace the oversight and judgment needed by those who own the institution's financial crimes compliance efforts.

The working group would be responsible for gathering all relevant documentation regarding how the institution manages its financial crimes risk. With oversight from the CCO, the working group would typically gather all relevant documentation which may include the institution's:

- AML, sanctions, and ABC risk assessments
- Other risk assessments for context such as operational and fraud risk assessments and the GRC assessment to the extent additional financial crimes risks are detailed therein
- Prior regulatory exam findings, internal audit findings, and consultant findings specific to elements of the financial crimes programs
- An institutional regulatory risk matrix if it exists and is relevant.

Furthermore, as part of its current-state assessment, the working group would also identify the strategic individuals within the institution that must be interviewed to better and more deeply understand the existing compliance approaches across financial crimes including existing risk management processes and controls.

Prior exam findings, internal audit findings, and consultant findings that are specific to financial crimes should be reviewed and considered. If an institution has a developed regulatory risk matrix that pertains to financial crimes, it can be very relevant and worthy of review.[7] The working group would also want to strategically identify those stakeholders that should be interviewed in order to better and more deeply understand specific financial crimes risks, existing risk management processes, and current controls.

Hopefully, current-state compliance initiatives are aligned with external regulatory and internal audit obligations. However, to the extent that they are not, this initiative can be a great opportunity to enhance management of such obligations in the future targeted financial crimes program. Any gaps, deficiencies, or weaknesses should be identified as considerations, even at this early stage. All components of the financial crimes framework should be assessed.

Tips: Do not go overboard or overengineer a current-state assessment. Working groups can become paralyzed by a desire to have a comprehensive understanding of the current state and feel unable to move forward until every stone is unturned. This is costly. Finding the appropriate balance for your institution between understanding and moving on to the design phase is essential, and compliance leaders must oversee and manage this balance through a carefully constructed and prioritized project plan.

[7] A regulatory risk matrix succinctly outlines what regulatory requirements currently exist for managing financial crimes compliance and describes why and how the institution is managing the requirements.

— Step 3: Design the framework

Executive leadership's commitment to the journey will largely drive the level of design work undertaken. At this stage, most institutions will draft a work plan that will serve as a "roadmap" for the journey. This will enable the working group to advise the compliance leader and executive leadership of the exact changes and efforts needed, as well as manage expectations for timeframes to complete.

Optimally, the work plan should create a step-by-step approach for the required changes. This typically includes upgrades to the technology infrastructure, compliance structure, and governance (compliance roles and responsibilities; escalation protocols), training, process controls, and more.

In addition, the work plan may also need to incorporate:

- A cultural change component. Cultural changes across the institution may need to occur, particularly if previously siloed compliance activities will now be coming together
- Consideration of each line of business' regulatory environment. When different lines of business are subject to different levels of regulatory expectation and scrutiny, it can be challenging if they must integrate under one centralized umbrella with stricter compliance requirements and/or protocols. Yet it is imperative that in the new financial crimes structure all employees involved in financial crimes risk management understand and accept the new approach.

A well-designed work plan should allocate time to perform compliance monitoring and Internal Audit testing before the program changes are final. Too often, the role of Internal Audit is an afterthought, and insufficient time is allocated for their test work. This can ultimately result in shifts to the deadline/timeframe and/or rushed Internal Audit test work, neither of which is ideal.

The work plan must contain essential milestones and the sources of information indicating achievement of those milestones. This is necessary for compliance leaders to develop the reporting dashboard for regular progress monitoring during the journey.

Perhaps most importantly, the institution's compliance leaders, executive leadership, and stakeholders should agree upon:

- Which individuals will design and implement the financial crimes program changes
- The governance oversight structure of the transformation, including the role of the board of directors
- The staffing model to be utilized during the transformation—which may include internal staff, external consultants, or a combination.

Since the institution owns its financial crimes risk, senior-level individuals must be involved enough for the institution to have confidence that risks will be managed and that new gaps in controls or processes will not result, exacerbating rather than mitigating risks.

Alongside the development of a work plan, institutions should conduct additional analysis as to the anticipated costs, benefits, urgency, resources, duration, and dependencies for each work stream and, at minimum, the compliance component level in order to better anticipate and plan for their needs.

Tips: Double- and triple-challenge whether goals, timelines, and cost estimates are realistic. Timelines often slip and costs rise as unforeseen dependencies occur, particularly when technology enhancements are involved. Frequently, compliance leaders find that necessary questions were not asked and, as such, relevant information was not known at the design stage. It may be helpful to strategize worst case scenarios and impacts in advance.

It is also beneficial to determine whether all relevant and appropriate stakeholders, including the board of directors and executive leadership, share the same vision for the future state and have a solid understanding of the planned transformation to be undertaken in order to avoid halts and restrategizing midstream.

— Step 4: Implement the future-state design

Since change is often disruptive within an organization, a well-defined communication plan can support a smoother implementation process and can reassure employees that the change is well-managed with an intent to minimize disruption to the business. For impacted employees, knowledge about what and when changes will occur is key.

Yet, over-communication should be avoided. For this reason, compliance leaders may enlist internal communications or marketing personnel to help them manage this aspect of the journey. These communications, along with the work plan previously developed, should help pave the way for a smoother implementation process. Collectively, the compliance team can determine the:

- Timing and cadence of communications
- Audience to be targeted
- Content of the communications, which could include reasons for the changes, anticipated benefits, and anticipated impact to employees.

For the remainder of this stage, the compliance leader's focus should be on implementing the desired changes—meeting the deadlines, articulating any dependencies or risks, and execution. At this juncture, project management support and accountability is essential. Involved personnel must clearly understand their tasks, have sufficient knowledge and experience to execute their portion of the journey, and feel comfortable escalating concerns to leadership.

Moreover, if new policies and procedures must be aggregated, old ones must be retired (in accordance with institutional protocols and as set forth in the work plan). This also applies to changes in technology, roles, and responsibilities and organizational structure. Tracking progress against the work plan on a regular basis will enable the project team and leadership to see progress, as well as manage costs.

Common challenges in implementation run the gamut and may include loss of key subject matter experts (whom also may have invaluable organizational knowledge) to attrition, lack of resources, difficulty managing all of the ongoing changes at once while continuing business as usual, and managing employee sentiments. It is likely, if the planning and design process was robust and reasonable, that these challenges can cause hiccups, but they should not derail the entire journey.

In the face of implementation challenges, compliance leaders must continue to lead and communicate. They should continuously seek solutions and ways to move forward, and, if they realize their internal teams are overwhelmed, they should escalate their need for additional support.

Tips: Stick to the design and the plan. When risks arise or dependencies slow down the process, compliance leaders should remain strong and strategic in order to adjust and realize a way forward.

— Step 5: Monitor for continuous enhancement

Once an institution has fully embedded its new financial crimes program, compliance leaders can sit back and admire what all their hard work has accomplished. Just kidding! If only it were that easy. Instead, compliance leaders must remain vigilant to identify new financial crimes risks and focus on further required enhancements as regulatory changes occur. And technology must be enhanced and innovative to address new opportunities for fraud and money laundering.

Financial crimes professionals can manage such risks by implementing ongoing financial crimes compliance monitoring and testing efforts within the second line of defense, which are sufficiently robust and structured to identify issues.

They should also continue to track potential regulatory changes that can impact their program through a sustainable regulatory change management program, inclusive of financial crimes. At this stage, maintenance and ongoing refinement become the focus.

As all good financial crimes compliance leaders recognize, and as Heraclitus stated, "There is nothing permanent, except change."

Tips: Recognize the journey is never over. The role of continuous monitoring and enhancement continues to be a part of business-as-usual. Staff with knowledge and experience are essential at this stage.

The financial crimes compliance framework and the journey steps are useful starting points for compliance leaders embarking on a journey towards greater financial crimes integration. They assist with understanding what the journey typically entails, the potential pitfalls and benefits, and industry leading practices that can be implemented for a smoother and more efficient journey.

Considerations checklist

When considering whether to undertake the journey to a more integrated financial crimes risk management approach, it is important to:

- **Collaborate and communicate** with stakeholders in the first, second, and third lines of defense, as well as the board of directors, to assess the benefits and costs of this type of restructuring and realignment of compliance initiatives
- Assess whether the journey would be valuable and be a compliance investment worthy of undertaking. Will it make your institution's compliance approach to these risks more effective, efficient, and agile? Will there ultimately be cost savings from this type of integration?
- Understand the projected costs to this type of restructuring and dependencies to that projection
- Understand the impact of this change on your people
- Consider the changes that will be needed to your technology infrastructure to support the new integrated structure and approaches, as technology can be a big investment
- Identify the right resources to complete, oversee, and support the journey
- Agree with stakeholders when the formal restructuring will be complete and business as usual will be in place
- Recognize the journey continues

About us

KPMG has extensive experience in assisting global clients throughout their compliance journey, helping them to realize the value of compliance, as well as greater program agility, effectiveness, efficiency, sustainability, and integration. KPMG works with clients to socialize large (and smaller)-scale transformational changes to their financial crimes programs or program components, including across multiple jurisdictions and lines of business. KPMG is distinctly positioned to provide insights into peer practices and to advise on a tailored approach that are right-sized for each client—considering the Institution's people, processes, technology infrastructure, data, risk appetite, and strategic goals.

We know what works and where the potential pitfalls are. While the journey often evolves, KPMG is a trusted adviser, supporting our clients every step of the way, sharing insights, and providing advisory support in a timely and cost-effective manner.

KPMG

Contact us

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

Acknowledgements: authored by Nicole Stryker and Jane Park; content and editorial contributors: Beth Rosenberg, Jennifer Collins, and Karen Staines (KPMG's CoE)

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

kpmg.com/socialmedia