The compliance investment

Realizing the value of compliance through greater
effectiveness, efficiency, and sustainability

kpmg.com

Amy Matsuo

Amy Matsuo is the national leader of KPMG LLP's (KPMG) Regulatory Risk practice, which advises companies on enterprise-wide compliance and other regulatory risk management issues. She leads the firm's multi-industry compliance transformation solution, serves as the program leader for the KPMG-sponsored Chief Compliance Officer Exchange, and is the service line lead for the U.S. Regulatory Center of Excellence.

Amy directs a team focused on regulatory and compliance assistance and preparedness. She also drives the firm's enterprise-wide compliance, program assessment and compliance transformation services for the financial services industry, including regulatory change, risk and control build and testing, risk governance, monitoring and reporting, and third-party management oversight and controls.

Amy received the 2014 Women Leaders in Consulting Award for client service. A frequent national and board presenter, she is both published and quoted on regulatory topics, enterprise-wide compliance programs, and fair banking and conduct risk practices. Additionally, she serves on the Women's Advisory Board of KPMG and is a member of its thought leadership committee. She also is on the national nonprofit board of One Simple Wish. She holds a Master of Public Policy degree from Georgetown University and a Bachelor of Arts degree from the University of Pittsburgh.

Richard H. Girgenti

Richard Girgenti is the U.S. and Americas leader for KPMG's Forensic Advisory Services and a member of the firm's Global Forensic Steering Group. He serves as the executive sponsor for the KPMG compliance transformation initiative and the KPMG-sponsored Chief Compliance Officer Exchange.

Richard has more than 40 years of experience conducting investigations, both nationally and globally; helping clients assess, design, and implement compliance programs; and providing fraud risk management advisory services to public and private corporations as well as to federal and state government entities and not-for-profit organizations. Prior to joining KPMG, Richard served as New York State Director of Criminal Justice and Commissioner of the Division of Criminal Justice Services. He was also a state prosecutor in the Office of the Manhattan District Attorney.

Richard is the co-author of two books: *The New Era of Regulatory Enforcement: A Comprehensive Guide for Raising the Bar to Manage Risk* (McGraw-Hill, April 2016) and *Managing the Risk of Fraud and Misconduct: Meeting the Challenges of a Global, Regulated and Digital Environment* (McGraw-Hill, March 2011). He holds a Juris Doctor degree from Georgetown University Law Center and a Bachelor's degree from Seton Hall University. He is a Certified Fraud Examiner.

Organizations today are challenged to address a confluence of regulatory and business changes that are putting new demands on compliance. The pace of regulatory change, convergence in global regulation, and competition from new market entrants that is driving increased consumer and technology demands have created a complex environment for compliance leaders across all industries. While financial services firms have notably faced a new wave of regulation since the 2007–2008 financial crisis, organizations in other industries have also felt the impact of a proliferation of new rules that affect nearly every part of their operations and influence their strategic decisions. Adding to this challenge is the risk of reputational damage and significant financial penalties that frequently accompany compliance failures.

For some organizations, compliance costs and inherent risks have dictated significant changes in product offerings and business operations. However, many are now viewing compliance as an investment and not simply as a cost. These organizations are realizing that business and operational value, such as better quality data and an improved customer experience, can be derived from anticipating risks and meeting regulatory requirements. This makes compliance an increasingly integrated part of the business investment strategy.

These changes have also elevated the stature and authority of the chief compliance officer (CCO) and increased the importance of effective governance, proactive risk management, and the need for continual compliance improvement. CCOs sit at the center of a compliance framework that demands the ability to work across functions and provides an opportunity to look at the breadth of risks facing their organization. This means that compliance should ideally be integrated across the business and positioned to contribute to business decisions and adapt to the changing business and regulatory environment. With greater integration and agility as the goals, compliance leaders can take immediate steps to enhance compliance effectiveness, efficiency, and sustainability.

Advancing in the compliance journey
A framework for compliance encompasses multiple components that drive prevention, detection, and response across the three "lines of defense." In a compliance framework, the business process owners are the first line of defense, compliance and centralized risk management functions are the second line of defense, and internal audit is the third line. Each line plays an important role in the organization's overall compliance framework and governance. The three lines

of defense model aids organizations in promoting compliance agility, identifying emerging risks, and clarifying the compliance program's strengths and weaknesses.

KPMG LLP (KPMG) has developed a proprietary compliance program framework that consists of eight program components, with culture and accountability at the core. 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 requirements and guidance from cross-industry regulators and leading compliance initiatives.

The importance of culture and tone from both the top and middle management should not be underestimated. Leading compliance programs that are plagued by cultural issues will still have problems. Similarly, a good culture can help organizations minimize misconduct while reducing the impact of compliance issues.

Regardless of the maturity of an organization's compliance framework across all eight program elements, compliance leaders recognize that their organizations need to improve in order to derive greater compliance value through increased effectiveness, efficiency, and sustainability. For each program element, organizations should determine their target state using a scale of 1 ("fundamental") to 5 ("advanced"). As organizations journey along the continuum, they tend to focus more on prevention and detection and less on response, allowing them to move toward viewing compliance as an investment and realize significant savings. Organizations further in their journey also transition to greater program centralization, integration, and sustainability.

Program continuum

5.0 Advanced compliance

3.0 Intermediate compliance

1.0 Fundamental compliance
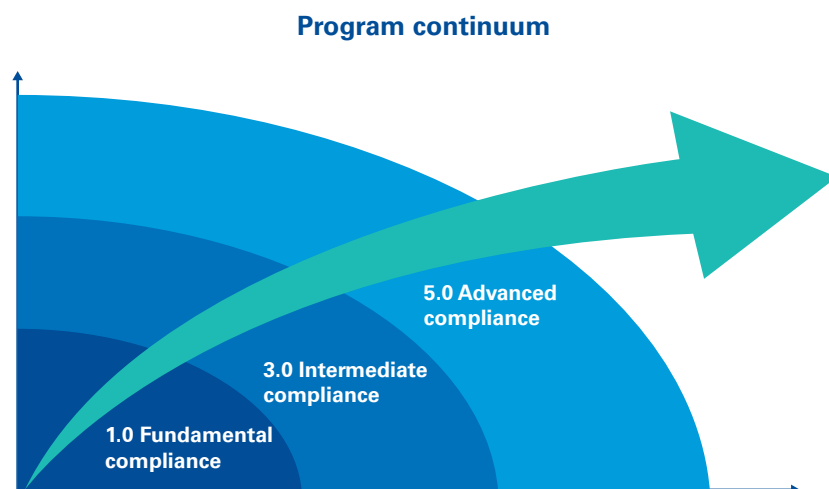
Larger organizations, for instance, often have a large number of regulatory issues. The cost of self-identification, auditing, and investigations for these issues can be immense. However, a reduction in the number of issues can bring significant savings.

For most organizations, the compliance journey will be a continual evolution and alignment between regulatory requirements and expectations as well as the organization's risk profile, culture, strategic and financial objectives, and business and operating models. For some, the length of the journey may depend on funding or the perception of the need to evolve further. For others, extensive transformation may be necessary simply to meet regulatory requirements. Further, the compliance journey often varies depending on the organization, its history, legacy structure, its prior experiences, industry, business activities, and future goals. Nonetheless, the journey represents an opportunity for all organizations to further integrate compliance requirements throughout the organization in a sustainable way and to identify new ways to gauge effectiveness and enhance efficiency.

Focusing on effectiveness, efficiency, and sustainability

Compliance leaders across industries are focused on assessing and enhancing their compliance effectiveness in response to regulatory requirements and expectations. This includes ensuring that they have a strong compliance culture embedded throughout the organization and that they are able to demonstrate to their boards and regulators that they understand and can manage their compliance risks. In addition, compliance leaders in organizations with more mature programs are also attentive to the need to improve the sustainability and efficiency of their programs.

While many compliance leaders are beginning to realize the value of their compliance investment through this focus on effectiveness, they often struggle with how to evaluate it. Many rely on internal metrics for insight into the effectiveness of their programs, including year-over-year improvement and how well they are filling self-identified compliance gaps and inefficiencies, as well as through an external analysis against peers. However, these may not be the most useful metrics given an organization's risks and strategic goals. Furthermore, compliance leaders recognize the limits of one-dimensional statistics, such as feedback from customers and regulators or decreasing fines. While these metrics provide some insight, they do not generally enhance an organization's awareness of its actual compliance effectiveness.

In response, compliance leaders are increasingly pursuing multidimensional metrics that link operational performance with compliance as well as metrics that can provide a deeper understanding of the organization's compliance effectiveness. Multidimensional metrics, for example, can enable an organization to better understand the root causes of issues related to retention, engagement, and attitude; the time needed to close audit issues and the number of repeat issues; and client satisfaction or complaints at the business unit level. These metrics also provide insights into compliance effectiveness.

Further, leaders are seeking data and analytics and other forward-looking predictive measures, as well as utilizing behavioral science indicia, to assess compliance trends and to enhance their understanding of emerging risks and potential misconduct. Examples of such forward-looking metrics

Case study: Beginning the compliance journey

A large U.S. regional financial institution faced regulatory pressure to enhance components of its compliance program. Regulators questioned the institution's enterprise-wide risk assessment, data integrity, technology infrastructure, governance oversight, and overall ability to manage certain compliance risks. The board of directors and compliance leaders across the organization recognized the need to improve their compliance activities as well as the importance of embedding any changes in a sustainable way. The bank, however, struggled to execute improvements and often found itself in a reactive mode.

The bank sought guidance to supplement its team's knowledge and efforts, identify gaps and risks in the program changes, and provide feedback that could help the organization realize a more strategic and risk-based approach to program changes. In the first steps of its multi-year compliance journey, the bank hired compliance leaders with broader experiences than those at many regional banks; transformed a number of data systems; refined its key risk indicators and key performance indicators to garner more refined metrics on program effectiveness; and enhanced the accountability of each line of defense for compliance. This resulted in greater awareness of its compliance risks and gaps across the enterprise, improvement in its internal control structure, and both strategic and tactical prioritization of enhancements in order to realize the greatest value from its investment.

might include a "click rate" that measures the number of employees who have read a particular policy, or tracking minor employee misconduct as an indicator of potentially more serious future misconduct.

In addition, certain metrics gleaned from employee surveys, cultural assessments, or focus groups can demonstrate how the compliance program is deployed within an organization and highlight the soundness of its design and execution. Assessments, for example, can also provide insights on cultural issues across the enterprise or on compliance bypasses that would not necessarily be caught through the other metrics.

While there are no universally accepted definitions of what makes a compliance program effective, and there is no one metric for evaluating effectiveness, the pillars of an effective compliance program are sound design and execution, timely and proactive responses to compliance issues, and readiness for regulatory change.

– **Sound design and execution:** Sound design and execution is the foundation of effective compliance. This is demonstrated when the program works as intended and recurring issues decrease over time. To assess design and execution, many compliance leaders look at their key risk indicators (KRIs) year over year or at surveys of targeted employees. They typically also consider the Committee of Sponsoring Organizations' (COSO) internal controls framework and guidance and measure their program against the seven topics set forth in the U.S. Federal Sentencing Guidelines. Regulators in certain industries have developed industry-specific guidance.

– **Timely response to issues:** While misconduct, gaps, and other issues can still occur regardless of the strength of an organization's compliance program, how an organization responds to a problem or crisis reflects its compliance effectiveness. A critical part of this response is the ability to implement a sustainable process to self-identify and self-report to regulators potential or alleged misconduct in advance of regulatory scrutiny. In addition, organizations should have processes for receiving and resolving broader issues, including consumer complaints.

– **Readiness for regulatory change:** Readiness for regulatory change requires organizations to both anticipate regulatory changes and respond quickly to comply. This includes revisions to its internal infrastructure and approaches.

In addition to effectiveness, organizations with more mature compliance efforts often find that the next step in their compliance journey—and a key to realizing a return on their investment—is making compliance more efficient and sustainable. Efficient compliance can address an organization's many regulatory mandates through a common set of controls that may require new automated, enterprise-wide controls to replace multiple or compensating controls within business units. This can be especially important for decentralized organizations and organizations that operate under multiple regulatory jurisdictions and face growing challenges in tracking and managing regulatory changes. Additionally, sustainable compliance requires compliance leaders to demonstrate effectiveness throughout the supervisory cycle as well as repeatable processes for an external consultant or audit assessment. Given staffing pressures and recent high attrition rates, embedding sustainable processes is increasing in importance.

Identifying compliance enhancements

While many organizations understand the need to continually advance in their compliance journey, there are several actions compliance leaders can take immediately to move toward greater agility and proactive compliance management while enhancing their compliance effectiveness, efficiency, and sustainability.

Review the "strategic" vision for compliance:
Compliance leaders should determine if the current compliance approach is meeting the organization's needs. This includes determining if it is working with the business or if it is perceived to be an obstacle or a redundant exercise. For compliance to be effective and sustainable, it must be aligned and integrated with the business. Helping to ensure that compliance is involved early in key decisions and is a partner of the business can help to reduce such issues.

Further, it is imperative that organizations have an understanding and vision for their compliance program that considers their existing and desired program structure, supporting technology, and the coordination and communication lines that are needed to enhance effectiveness, sustainability, and efficiency. Many organizations continue to question if their structure is well designed and implemented to identify and escalate compliance risks or if the structure needs changes, including further centralization. While there is no "one-size-fits-all" approach to a compliance structure, organizations that fully understand their organizational regulatory requirements—including emerging regulatory changes and challenges, history, people, technology, control coverage, and risks—are well-positioned to assess if changes to the program infrastructure would be valuable and have a significant impact on organizational compliance.

Importantly, compliance officers should be attuned to the fact that enhancements to one compliance program area—such as its data analytics and technology or governance and culture—can have real and significant impacts on other compliance program components. For example, enhancing data analytics to include new testing data can impact the organization's risk assessment, issues management, and many other compliance program components. Given the interconnected nature of a compliance program, regulators are increasingly seeking a single and consistent compliance view across organizations. The program must create synergy and program components must work together in design and execution.

Perform an enterprise-wide risk assessment:
Compliance leaders and the board of directors need enterprise-wide risk assessments in order to have a holistic understanding of the organization's risk universe, the materiality of those risks, and, in particular, its systemic risks. Organizations increasingly recognize the importance of an annual enterprise-wide risk assessment, and many use their risk assessments as a strategic input for their audit plan and program enhancement decisions. Further, regularly scheduled risk assessments can also help compliance leaders improve their resource allocations and staffing models to align compliance more efficiently with their risks and needs and to produce a more effective result.

However, assessments are often focused on specific regulations, such as the Foreign Corrupt Practices Act or sanctions, rather than on serving as a holistic assessment of the overall compliance program. Alternatively, the risk assessments may be performed by the business units with limited aggregation at the enterprise-wide level. When this happens, systemic risks across the enterprise and across regulations may not be apparent. For that reason, it is vitally important that compliance leaders have a process in place for aggregating enterprise-wide quantitative and qualitative data that can then be communicated to the board.
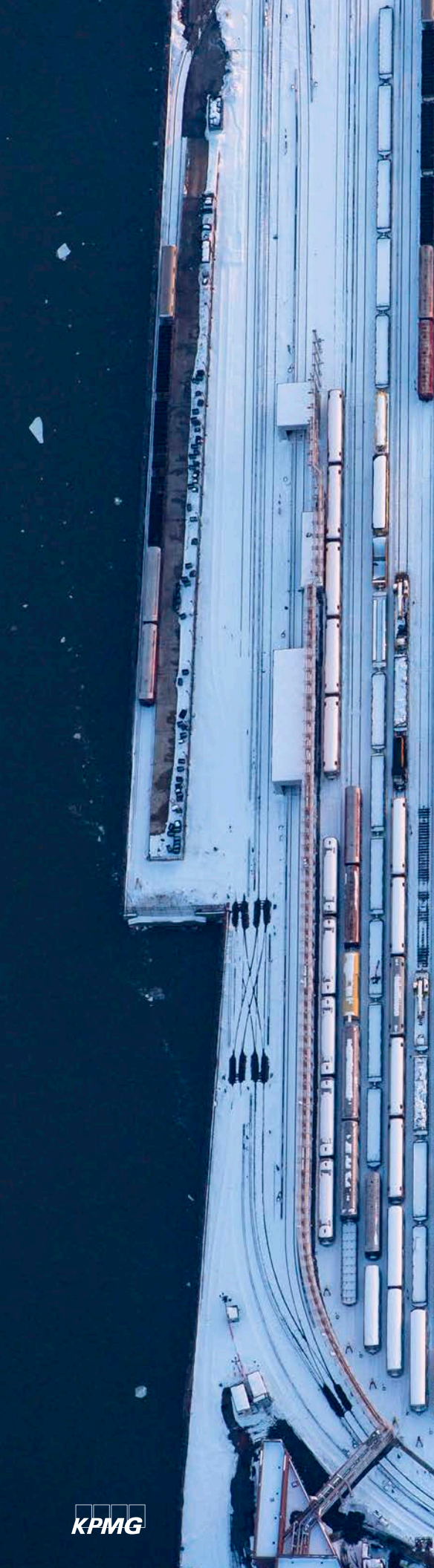
The enterprise-wide risk assessment should contain sufficient detail for compliance leaders to evaluate the organization's inherent risks, mitigating controls, and residual risk. The CCO can then use this assessment to target elevated or higher risk areas more effectively for enhancement, to refine the annual compliance monitoring plan, and for internal audit to leverage in its testing plan. By providing a thorough report to the board on control gaps and residual exposure across the organization, the board is better equipped to evaluate if the organization's residual risk is consistent with its risk tolerance and desired risk profile, or to determine what changes to the business or strategy are needed to bring residual risk back into alignment.

Help ensure an effective three lines of defense: Organizations can also evaluate if their three lines of defense are being used effectively and seek to understand the rationale for any overlap. The three lines of defense model aids in promoting compliance agility, identifying emerging risks, and in clarifying the compliance program's strengths and weaknesses. Organizations that apply this model to their compliance approach use it to reduce risk, strengthen culture and behavior, and enhance governance, organization, and infrastructure.

As a first step in this evaluation, compliance leaders should confirm that roles and responsibilities for each line of defense are clearly defined and appropriately aligned with each line's mandate. Where overlaps exist, leaders should consider if this is intentional or if processes can be streamlined. One particular area of focus for compliance leaders today is on further establishing the parameters for the first line of review, including for conducting quality assurance reviews and monitoring.

In further developing compliance responsibilities for business units and operations, compliance leaders find value through a more preventive approach that creates greater accountability and reduces business disruptions. For example, this enhancement of the organization's preventive controls also tends to create greater accountability within the line of business and often leads to more immediate identification and escalation of risks. Organizations should also consider the communication and coordination protocols that should exist throughout the planning and execution stages. As a better practice, compliance leaders should also evaluate where direct and indirect compliance coverage will exist among the lines of defense, which areas of compliance will be covered centrally, and which will be decentralized with associated standards.

One indicator of whether an organization is maximizing its three lines of defense is if it has a harmonized and common set of controls. With a common set of controls, an organization can develop better practices around a single set of controls that can be easily modified, allowing compliance to adapt more quickly as the regulatory environment evolves.[1] This is characteristic of more mature compliance programs and is nonetheless a challenge for many organizations with multiple and incompatible technology systems and with a compliance program that is less integrated across the business lines.

[1] *Sustainable Compliance: How to Align Compliance, Security and Business Goals,* NET IQ (2012).

During this evaluation, compliance leaders should also consider their organizational mandate for compliance and the compliance coverage needed. Since, in some sense, everything can become compliance when regulations are involved, compliance leaders benefit from clearly defining the compliance matters within the compliance function's mandate, the responsibility of information technology (IT), and the responsibility of the business or operations (with compliance input as needed). For example, does compliance own cybersecurity or environmental compliance? What about investigations? Such analysis similarly helps organizations to better understand and document its compliance program and coverage.

Assess the organization's "culture of compliance":
A "culture of compliance" requires an organization to demonstrate the values of integrity, trust, and respect for the law.[2] Regulators are increasingly focusing on an organization's compliance culture and recognizing it to be an essential preventive control against many forms of misconduct. Regulators often view the lack of a culture of compliance as the root cause of misconduct within an organization.

Transforming an organization's culture, however, is a long-term investment. It requires the commitment of the most senior leaders and often presents these leaders with unexpected challenges and difficult decisions. To embed a culture of compliance, an organization must have established guidelines, and employees at all levels must be held accountable in accordance with these guidelines and without exception. The board and senior management must not only establish the core values and expectations for their organization but must also act consistent with those values and expectations at all times.

Compliance leaders should also periodically confirm the existence of the compliance culture, ensuring that sub-cultures do not negate or hinder their compliance culture, and determine if the culture is embedded consistently across its business and operational units. One way to accomplish this is through a "cultural assessment." This assessment typically enables compliance leaders to understand whether people are comfortable with the culture of the organization, how employees view organizational justice, how management decides ethical issues, and if employees are willing to identify issues without fear of retaliation. All of these factors are important indicators of the compliance culture across the organization.

Assess current technology: Technology and data analytics are essential tools for organizations in preventing, detecting, and even responding to potential compliance misconduct.

In recent years, organizations have faced a significant transition to digital content and records as well as changes to their core platform systems. They have also faced the need to further aggregate their compliance risk indicators, including with respect to their third parties, investigations, culture, and internal monitoring and audit efforts. In addition, depending on the industry, organizations may be challenged by regulatory requirements to link their compliance performance to their operational metrics such as employee behavior and anomalies in activity (including in distribution channels or customer trades). Organizations are also increasingly concentrating on refining their predictive indicators, which necessitate certain technology functionality as well.

Yet, many organizations still have legacy technology systems or disparate systems across the organization that are a consequence of organizational expansion or mergers and acquisitions. Importantly, existing technology may also lack the requisite functionality to link compliance to operational metrics and aggregate predictive metrics. To address these changing market and operational circumstances, organizations are increasingly implementing tools for governance, risk management, and compliance (GRC); case management; or other embedded technology to further support all components of their compliance program in an integrated and sustainable fashion. This includes automating transaction monitoring across their organization; aggregating data and documentation in one central repository, including for third-party risk management; applying consistent risk ratings to activity and/or parties; accessing data for meaningful KRIs and key performance indicators (KPIs); tracking ongoing monitoring and reviews; automating aspects of monitoring; and addressing regulatory changes and exception reporting.

These operational changes require compliance to be involved in system design and changes. Defined user acceptance testing (UAT) and validation of any data flows, system functionality, and translation of unstructured data to structured data should also be planned and executed. Further, these changes necessitate at least a certain level of transition to more centralized and integrated technology infrastructure across the organization as well as to more robust data analytic capabilities. As organizations shift to greater automation for selected data and system processes, compliance leaders should be alert to the impact of this on other components of their compliance program such as their risk assessments, reporting, and governance. They should also integrate this information in the annual risk assessment, enabling the board and senior leaders to better understand compliance risks and to identify compliance program enhancements for prioritization.

---

[2] The Financial Industry Regulatory Authority (FINRA) defines 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."

Proactively address regulatory change: Managing regulatory change is a significant challenge that can put organizations in a reactive position, especially when an organization operates in diverse businesses, in highly regulated industries, or in multiple jurisdictions. However, organizations in today's ultra-competitive market simply cannot afford to respond ad hoc to regulatory change. An ad hoc approach typically limits the time an organization has to assess needed changes and arrive at the right solution for their organization. For this reason, organizations must be able to adapt proactively to the changing regulatory environment.[3]

By establishing a regulatory change management process that identifies and tracks potential regulations and evaluates their impact on the organization, compliance leaders are better positioned to address these changes when they come to fruition. Vendor tools can also help automate some of this process, supplemented by internal employee resources. In addition, a leading practice among many businesses is to maintain a real-time, continuous inventory of global regulatory obligations and regularly scan the regulatory horizon to identify new and emerging changes or triggering events.

A regulatory change management process should provide for an aligned view across portfolios in order to understand the global interdependencies among other strategic initiatives and regulations. In addition, organizations should utilize external industry thought leadership to stay ahead of regulatory automation trends as well as leading practices to further develop their understanding of divergences across regulations and jurisdictions. This, combined with a more robust knowledge of the organization's regulatory environment, can help improve operational efficiency and enhance cross-border coordination. Because regulatory changes often require updates to organizational systems, processes, and structure, approaching these changes collectively and in a proactive manner is an opportunity for increased effectiveness and efficiency. Organizations can also implement a consistent global methodology that is administered by a global program office.

---

[3] *Sustainable Compliance: How to Align Compliance, Security and Business Goals*, NET IQ (2012).

Conclusion: Realizing the value of compliance

Viewing compliance as an investment, and not simply as a cost, can help measure its return during ongoing compliance improvements while propelling the organization toward greater effectiveness, sustainability, and efficiencies in its compliance efforts. Organizations can do this by considering the business and operational value—in addition to the compliance value—that this investment provides. For example, while the investment in technology, cultural change, or strategic evaluations of the program is a real cost, it can result in significant process improvement, control enhancements, and improved customer experiences. While these can be hard to quantify, they are impactful nevertheless.

For many organizations, the journey of developing compliance from what it has been to what it needs to become can be a major undertaking. Organizations find it challenging to address all of the significant impacts to the organizational structure, processes, and technology that people are used to working with. Convincing or aligning people in the compliance journey can meet with resistance, as employees question why the changes are needed and question the value from such adjustments. In addition, migrating data or integrating systems is a complex process with significant costs. The culture of the organization itself can also be a hurdle, as different business units in many organizations are difficult to align.

However, compliance is an ongoing process that requires continuous oversight and continuous improvement. As businesses are pressured to become more agile and cost-effective in response to changing market conditions, leaders must likewise improve their compliance agility, adaptability, efficiency, and sustainability. This journey must make compliance part of the core business team that considers systems, products, and business changes. Persisting in this journey can help organizations stay ahead of regulatory change and adapt to a complex business environment. In taking the actions outlined in this article, compliance leaders will be better positioned to refine their compliance approach more strategically and to realize increased effectiveness and improved efficiency and sustainability.

How KPMG can help in your compliance journey

KPMG helps organizations across industries further develop and enhance their compliance program with the intent to help increase effectiveness and efficiency, expand compliance integration, and enhance strategic business decision making.

KPMG's services are customized according to an organization's regulatory requirements, objectives, business, operations, and jurisdictional reach. We help organizations fundamentally reassess and retool their compliance governance, compliance culture, and business and risk operations. This includes helping our clients align their compliance programs to the specific requirements of their industry and jurisdiction, anticipating regulatory change, and enhancing their understanding of the practices of their peers.

KPMG's customized approach allows us to evaluate an organization's compliance risk culture; recommend and assist in implementing an enhanced compliance risk assessment; assess the current state of an organization's compliance program; and recommend a target operating model using KPMG's proprietary maturation criteria. This criteria incorporates our industry knowledge for either a broad or targeted industry-based benchmark that is sized for the organization and uses the relevant peer-group or sector standards.

Contact us

Amy Matsuo
Compliance Transformation
Solution Leader

U.S. Financial Regulatory Risk Lead
T: 919-380-1509
E: amatsuo@kpmg.com

Rich Girgenti
Compliance Transformation
Solution Executive Sponsor

U.S. and Americas Leader for
KPMG Forensic Advisory Services
T: 212-872-6953
E: rgirgenti@kpmg.com

Additional Contributions

Compliance Transformation Industry Leaders

Kari Greathouse – Technology, Media and Telecommunications Lead Principal

Stacey Guardino – Insurance Lead Partner

Tim Hedley – Consumer Markets, Diversified Industrials Lead Partner

Julie Luecht – Energy Lead Principal

Anthony Monaco – Government Lead Partner

Jennifer Shimek – Healthcare, Life Sciences Lead Principal

Compliance Transformation Support Team

Julie Gerlach – Managing Director

Nicole Stryker – Director

Phil MacFarlane – Associate Director

kpmg.com/socialmedia