Reprinted from COMPLIANCE WEEK

The compliance investment

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

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.

Chief Compliance Officers (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.

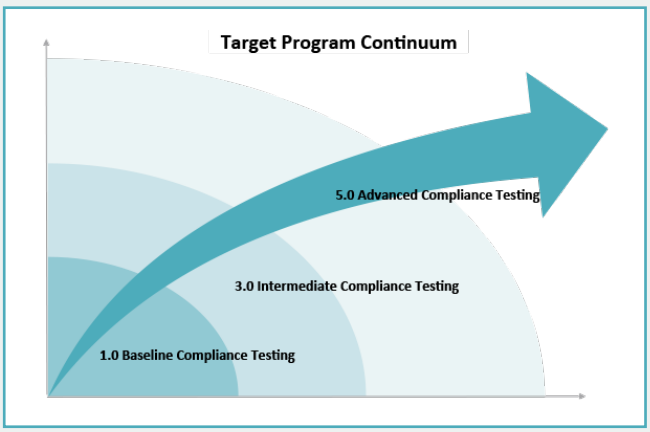
The compliance journey

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 of defense 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.

Regardless of the maturity of an organization's compliance framework across all eight program elements, compliance leaders recognize that their organizations need to improve to derive greater compliance value through increased effectiveness, efficiency, and sustainability. For each pro-

gram element, organizations should assess and 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.



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.

Identifying compliance enhancements

While many organizations understand the need to continually advance in their compliance journey, there are several actions compliance leaders can immediately take 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. Ensuring 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. 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 impactful on organizational compliance.

Importantly, compliance leaders must be attuned to the fact that if they enhance one area of the compliance program—such as their derived data analytics or governance—this can have 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.

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 more efficiently align compliance 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 serving as a holistic assessment of the overall compliance program. Alternatively, risk assessments may be performed in silos by 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 quantitative and qualitative data enterprise-wide, which can then be communicated to the board. By providing a comprehensive 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.

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. As a first step in this evaluation, compliance leaders should confirm that roles and responsibilities for each line of defense in executing their program reviews 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 by 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 the business units' and operations' compliance responsibilities, compliance leaders find value through a more preventive approach that creates greater accountability and minimizes business disruptions.

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 what compliance matters are within the compliance function's mandate versus what is the responsibility of Information Technology (IT), 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. 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.

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 the 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 upon 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, 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.

These operational changes require compliance to be up front in the design of systems 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 ro-

bust 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.

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. Yet organizations in today's ultra-competitive market simply cannot afford to be in a position of responding ad hoc to regulatory change. This 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.[1]

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. 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. This can improve operational efficiency and enhance cross-border coordination across multiple jurisdictions.

Conclusion: The value of compliance

Viewing compliance as an investment, as opposed to as simply a cost, can help measure its return during ongoing compliance improvements, while simultaneously propelling the organization toward greater effectiveness, sustainability, agility and efficiencies in its compliance efforts. For example, while an 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, which can be hard to quantify, but impactful nevertheless.

Furthermore, 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. In taking the above actions, compliance leaders will be positioned to more strategically refine their compliance approach and to realize increased effectiveness and improved efficiency and sustainability.

AMY MATSUO

Amy is the national leader of KPMG's Regulatory Risk practice that advises companies on enterprise-wide compliance, safety and soundness, broker/dealer, asset management, consumer compliance and other regulatory risk management issues. In addition to being the Regulatory Risk national partner, she leads the firm's multi-industry compliance transformation solution.

ADDITIONAL CONTRIBUTIONS

Contributions and insights also provided by Richard Girgenti (U.S. and Americas Practice Leader, KPMG Forensic), Julie Gerlach, Nicole Stryker, Stacey Guardino, Jennifer Shimek, Julie Luecht and Tim Hedley.

ABOUT KPMG

KPMG LLP, the audit, tax and advisory firm, is the U.S. member firm of KPMG International Cooperative ("KPMG International"). KPMG is a global network of professional firms providing Audit, Tax and Advisory services. We operate in 155 countries and have more than 174,000 people working in member firms around the world.

1 Sustainable Compliance: How to Align Compliance, Security and Business Goals, NET IQ, 2012.