The

compliance
investment

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

> **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.**

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, competition from new market entrants, and increased consumer and technology demands have created a complex environment for compliance leaders across all industries. 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. With greater integration and agility as the goals, compliance leaders can take immediate steps to enhance compliance effectiveness, efficiency, and sustainability to further realize the value of compliance.
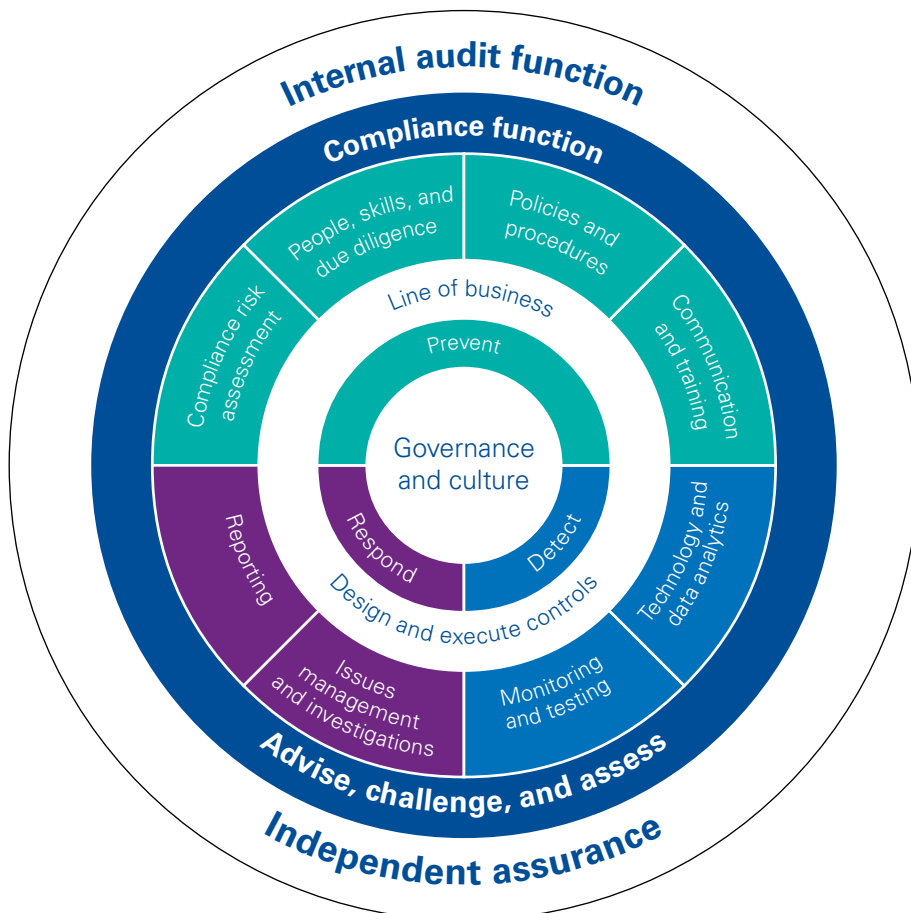
The compliance journey

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. 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 (US) has developed a proprietary compliance program framework that consists of eight program components, with culture and accountability at the core (see Figure 1).

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

Figure 1: KPMG's compliance program framework

Internal audit function
Compliance function
People, skills, and due diligence
Policies and procedures
Compliance risk assessment
Communication and training
Line of business
Prevent
Governance and culture
Technology and data analytics
Reporting
Respond
Detect
Design and execute controls
Issues management and investigations
Monitoring and testing
Advise, challenge, and assess
Independent assurance

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. As organizations journey along the continuum, and shift their focus to more prevention and detection efforts, they also tend to transition to greater program centralization, integration, and sustainability. They thus derive a greater value from their investment.

For most organizations, the compliance journey remains 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

As compliance leaders contemplate how to advance in their compliance journey, there are several actions that compliance leaders can consider 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. It is imperative that compliance leaders 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. This includes alignment and integration with the business, as well as partnering with the business throughout key decision-making periods.

In addition, compliance leaders must be attuned to the fact that if they enhance one area of their compliance program this can have significant impacts on 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 an enterprise-wide risk assessment 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.

If compliance leaders conduct assessments in silos or focused on specific regulations, with limited aggregation enterprise-wide, systemic risks across the enterprise and across regulations may not become apparent. For that reason, it is vitally important that compliance leaders have a process in place for aggregating quantitative and qualitative data enterprise-wide and to identify residual exposure *across* the organization. This is also essential for the Board's evaluation of whether 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. Compliance leaders should confirm that roles and responsibilities for each line of defense are clearly defined and appropriately aligned with each line's mandate, and that the rationale for any overlap in responsibilities is clearly understood. One particular area of focus by compliance leaders today is on further defining the first line's role in monitoring and quality assurance reviews. By allocating monitoring and review responsibilities to the first line, compliance leaders craft a more preventive approach to compliance, and find value in instilling greater accountability.

As part of its three lines of defense analysis, compliance leaders can also benefit from clearly defining what compliance matters are within the compliance function's mandate versus what is the responsibility of operational and business units (with indirect compliance input and coverage as needed). 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

> "This includes alignment and integration with the business, as well as partnering with the business throughout key decision-making periods."

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, 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 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.

Assess current technology: Technology and data analytics are essential tools for organizations in preventing, detecting, and 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 also need to further aggregate their compliance risk indicators and may be challenged by regulatory requirements to link their compliance performance to their operational metrics. 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 support their compliance program.

These operational changes require compliance to be up front in the design of systems and changes. Further, these changes necessitate a transition to more centralized and integrated technology infrastructure across the organization as well as to more robust data analytic capabilities.

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 this approach 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.

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 effectiveness and efficiencies including process improvement, control enhancements, and improved customer experiences, which can be hard to quantify, but impactful nevertheless. In taking the above actions, compliance leaders will be positioned to refine their compliance approach and to realize increased value.

> **Organizations are also increasingly concentrating on refining their predictive indicators, which necessitate certain technology functionality as well.**

For more information:

Amy Matsuo
Partner, Regulatory Risk
KPMG in the US
E: amatsuo@kpmg.com