Bloomberg Law®

Corporate Law & Accountability Report™

COMPLIANCE

The Future of Compliance: Top 5 Investments to Prepare for the Future Today

BY AMY MATSUO

For compliance leaders, navigating today's regulatory landscape might seem like playing a game with constantly shifting goal lines. And, these changes will likely continue as the current U.S. administration pursues its plans to pullback various regulations on businesses.

While meeting new compliance requirements will be a short-run challenge that will require greater agility, compliance leaders will also need to focus on the future, working to continuously improve their compliance programs and foster greater alignment with their business strategy.

At the same time, stakeholders across the organization are seeking to increase the effectiveness and efficiency while cutting the cost of their compliance activities to further compete in an expanding digital and automated world.

Amy Matsuo is a Principal in KPMG LLP's Risk Consulting Practice and the National Leader of KPMG's Regulatory Insights Practice with over 20 years of experience providing advisory services to large domestic and global organizations. The Regulatory Insights team drives value to KPMG clients and professionals on key regulatory and public policy developments and disruptors across all major industries.

What follows are the top five areas where compliance leaders need to focus to meet the challenges this year and beyond. Investment in these areas will allow organizations to identify and respond early to shifts and trends, enabling business, risk, legal, technology, and internal audit leaders to move beyond compliance to create value.

1. Culture

Culture is the foundation of compliance and it is jumping to the forefront of Board and executive agendas across all industries, prompting evaluations of their culture and a commitment to refinement enterprise-wide.

Senior leadership, in conjunction with compliance and human resource (HR) personnel and line of business executives, must establish and drive culture into all facets of the organization. This includes from the highest level employee to the entry level staff. Subcultures that do not align to the desired compliance culture must be weeded out.

Even in this current environment where organizations are automating more and more compliance processes, and further integrating their efforts, culture remains the number one preventive control. To be effective, including in an increasingly technological world, compliance leaders must bring compliance to life for its employees, encourage a speak-up mentality, and enhance employees' accountability for compliance.

To achieve this, collaboration with HR to identify practical ways to build compliance responsibilities into employee performance evaluation process, and address any potential barriers should take place. By incorporating compliance into employee performance process, including the awarding of bonuses and pay raises to those employees who are ambassadors of the compliance message, organizations reinforce the message that compliance counts, and that employee actions must align to the organization's culture and values. But compliance must also be woven into disciplinary protocols as well, requiring actions, such as warning letters, pay cuts, or even termination, for those who fail to act in ac-

cordance with compliance requirements and the culture.

In this area, it seems there is still work to do. According to a KPMG survey of chief compliance officers (CCOs), 39 percent said that they do not, or do not know, if employee compliance with policies and procedures is factored into performance and compensation evaluations.

But instilling the importance of compliance into the rank and file is only part of the compliance culture equation. It's also critical that disciplinary and incentive standards be consistently applied to high-level employees and leadership. Failure to do so sends the undesirable message that seniority and success can exempt you from following the rules, and undermines the culture of compliance.

Imparting a stronger sense of accountability among employees can also mean the organization will have to make some tough decisions to reinforce the compliance culture. Here are a few examples:

■ Clawing back executive compensation when it was earned through fraudulent or unethical behavior

■ Making enterprise-wide adjustments to the Performance Management System, including the incentive compensation structure to emphasize non-sales performance metrics or to eliminate or downplay sales goals and balance sales goals against employees compliance

■ Calling off a merger or acquisition transaction because leadership found that there was misconduct or unethical conduct underpinning the deal

Ultimately, an organization can have a sound compliance framework with all the right policies and procedures in place, but if individuals who break the rules aren't held accountable for their actions—particularly those in leadership—and the culture is bad- then the very foundation of compliance is compromised.

2. Operational integration

Regulators are increasingly spotlighting the need for operational integration within a compliance risk-management program. ''Operational integration'' means incorporating compliance into the business processes and into people's daily performance of their job duties.

Integrating compliance into the business operations improves the likelihood of an organization detecting a broad range of issues—from fraud, sanctions, theft, or asset misappropriation to cybercrimes and corruption. This is because integration positions organizations to access and aggregate data enterprise-wide, thereby enabling a more holistic evaluation of compliance risks, which may stem from the organizational culture, specific jurisdictions or business units, or other parties (such as employees, vendors, and suppliers).

Operational integration facilitates a more tailored, concerted and consistent approach to risk management. In addition, integration can result in:

■ improved data aggregation and more thorough data analytic capabilities

■ a more focused approach to managing risk across the organization

■ a common repository for data and a united technology infrastructure

■ heightened awareness and understanding of enterprise-wide risk by the board of directors

■ a strengthened control environment

■ cost savings as a result of reduction in complexity and duplication

■ enhanced ability to comply with changes to an organization's regulatory expectations

For integration to work, however, it needs to involve functions from across the entire enterprise, including HR, finance, legal, technology, procurement, and marketing. While many of these functions may not have traditional compliance roles and responsibilities, their position within the organization allows them to observe and offer information regarding gaps, weaknesses, or strengths in the organization's compliance program.

Some organizations find that a more centralized governance approach or a hybrid approach to managing compliance is best. This involves centralizing key compliance activities and processes at the enterprise wide level. In this way, silos are broken down and information can flow more freely, greater consistency in controls and processes across business units can be realized, and a more cohesive approach to compliance can be implemented.

3. Automation of compliance activities

Intelligent automation is increasingly being used by organizations to automate routine tasks, increasing efficiencies and lowering costs. As technological advances occur, organizations are starting to pivot from initial automation efforts in operational processes to compliance ones.

Automation helps compliance leaders respond to growing regulatory expectations, while reducing compliance costs, increasing enterprise-wide coordination, and contributing to more agile business strategies. It can be applied to cybersecurity, monitoring and surveillance, regulatory change management, regulatory reporting, third-party risk management, and importantly, the development of predictive analytics.

When looking to automate processes, it's essential to have an overall plan and determine which processes are best to automate and in what order. Here are some important considerations when identifying compliance activities to automate:

■ By starting at the finish line, and considering their organization's current state, compliance leaders can identify what steps need to be taken to bridge the gap. To evaluate compliance goals (and align to business goals), leaders should consider what their organization will need to look like across people, processes, and technology so they start building an appropriate infrastructure.

■ Often there are dependencies when it comes to automating certain processes and activities. These dependencies should be considered when ordering a planned automation. For example, if data integrity or accuracy need to be improved, that must be accomplished before the automation of a compliance activity can occur.

   ISSN 2330-6300

■ Tactical investments in technology should have long-term benefits for both compliance and the overall profitability of the business. Compliance leaders should coordinate and collaborate with the business when prioritizing automation initiatives.

■ When planning an automation project, compliance leaders need to evaluate the technology solutions available for each activity. They should compare vendors and determine whether to build, buy, or team with a technology provider. If an organization chooses to seek external services, the importance of understanding each vendor's offerings and how the solution's functionality/capabilities align with the organization's compliance goals and needs cannot be overstated.

Despite offering many benefits, new technology also has its own risks—such as algorithmic bias and insufficiently robust data. To have a successful implementation and rollout, organizations should embed their risk and compliance frameworks up front in the design phase of their automation technology implementation, and then revisit their effectiveness continuously throughout the lifecycle of their transformation and thereafter.

4. Risk assessments

As stated at the beginning, the compliance landscape continues to change. Therefore, regular compliance risk assessments, that not only ensure that regulations and internal requirements are being met, but which also survey the regulatory landscape proactively for future changes, are critical. Unfortunately, many CCOs are unaware of the effectiveness of their current state risk-assessment process, much less monitoring and tracking potential changes that could be quite impactful down the line. KPMG's 2017 survey of CCOs found that 24 percent of respondents either said that their organization's risk assessment processes didn't consider whether internal controls are designed appropriately and operate effectively or that they didn't know.

The critical role of sound risk assessments in compliance risk management was reinforced last year when the Fraud Division of the U.S. Department of Justice released a guidance document, ''Evaluation of Corporate Compliance Programs, containing specific questions that organization can use to evaluate their efforts. Among the questions are: does the organization have a ''risk assessment''; what methodology is used; what kinds of information and analysis are used in the process; and how does the risk assessment capture ''manifest'' risks.

As regulations continue to change and compliance expectations increase, organizations will need to develop ever more sophisticated risk assessments to understand and assess how they are mitigating their existing compliance risks, to further evaluate risk trends, and to anticipate compliance risk that may arise in the future.

To bolster the value of an annual risk assessment process, compliance leaders should consider implementing the following:

■ **Proactive management of regulatory change**: As a first step to proactively managing regulatory changes, which can create or intensify compliance risks, organizations can develop an inventory of the existing compliance requirements or obligations that apply to their businesses, products and services and the jurisdictions where they operate. Such an inventory is foundational to the compliance risk-assessment process and can aid in the identification of gaps and weaknesses in the control environment. It also empowers organizations to evaluate the impact of regulatory changes across their control environment.

■ **Refinement of their methodologies**: Regulators are interested in understanding organizations' methodology for identifying, analyzing, and addressing their compliance risks. A clearly documented methodology creates a blueprint for the execution of the compliance program that is sustainable and encourages consistent implementation. A strong methodology also sets forth parameters for reporting assessment results to the board in a digestible way, with guidelines for the level of data and information, which increasingly includes data from internal investigations, monitoring and testing, and root cause analysis outcomes. A strong and robust methodology helps to ensure the board is adequately informed with the right level of information to oversee the organization's risk management and tolerance.

■ **Establishment of a feedback loop**: It is valuable to discuss final compliance risk assessment results with those business and operation units that are involved. A feedback loop engages the first line in ongoing compliance risk management and provides business and operational Leaders with greater visibility of their compliance risks and how they fit and overlap across the enterprise. This in turn helps to instill greater accountability and ownership of compliance risk by the first line of defense.

5. Continuous Improvement

Effective risk assessments that uncover compliance gaps and weakness are only part of the process needed to maintain an effective compliance program today and into the future. Organizations must also continuously improve in their compliance efforts to ensure their control environment remains firm in the face of shifting goal lines - regulatory expectations and requirements and emerging risks and is responsive to risk trends. Monitoring, testing, auditing, and investigations play a significant role in the compliance program life cycle and aid compliance leaders in identifying ways to further minimize misconduct and continuously improve. Moreover, regulators expect organizations to have a robust testing program and, in turn, for those results to be used in the continuous improvement of the program.

Compliance leaders ought to continuously assess their efforts, including their:

■ Regular testing and audit efforts, including when changes to the organization's risk profile occur (including introduction of new products or services, changes to jurisdictional markets served, mergers or acquisitions, or changes to third-party relationships.)

■ Ongoing tracking of potential regulatory changes that have potential to affect their compliance activities.

■ Market changes and trends, including evolving technology, that could impact compliance efforts and change the firm's risk profile.

■ Root-cause analysis information and investigation outcomes, including from employee surveillance, third party monitoring and behavioral analytics in order to target heightened risks areas or parties.

■ Data that reflects the health of compliance efforts, and missing or needed data that can support more predictive analytics.

■ Potential gaps and tracking of remediation efforts.

Final Thoughts

By advancing integration and automation of compliance efforts, compliance leaders can realize a more holistic vision of their compliance risk, greater consistency in outputs, and expanded risk coverage and enhance their compliance infrastructure for the future. Further refinement of their compliance risk assessment, activities to reinforce culture including through greater employee accountability, and program improvements will also position compliance leaders and their evolving programs to remain ahead of, and positioned to comply with, regulatory expectations, not just in 2018, but beyond.

   ISSN 2330-6300