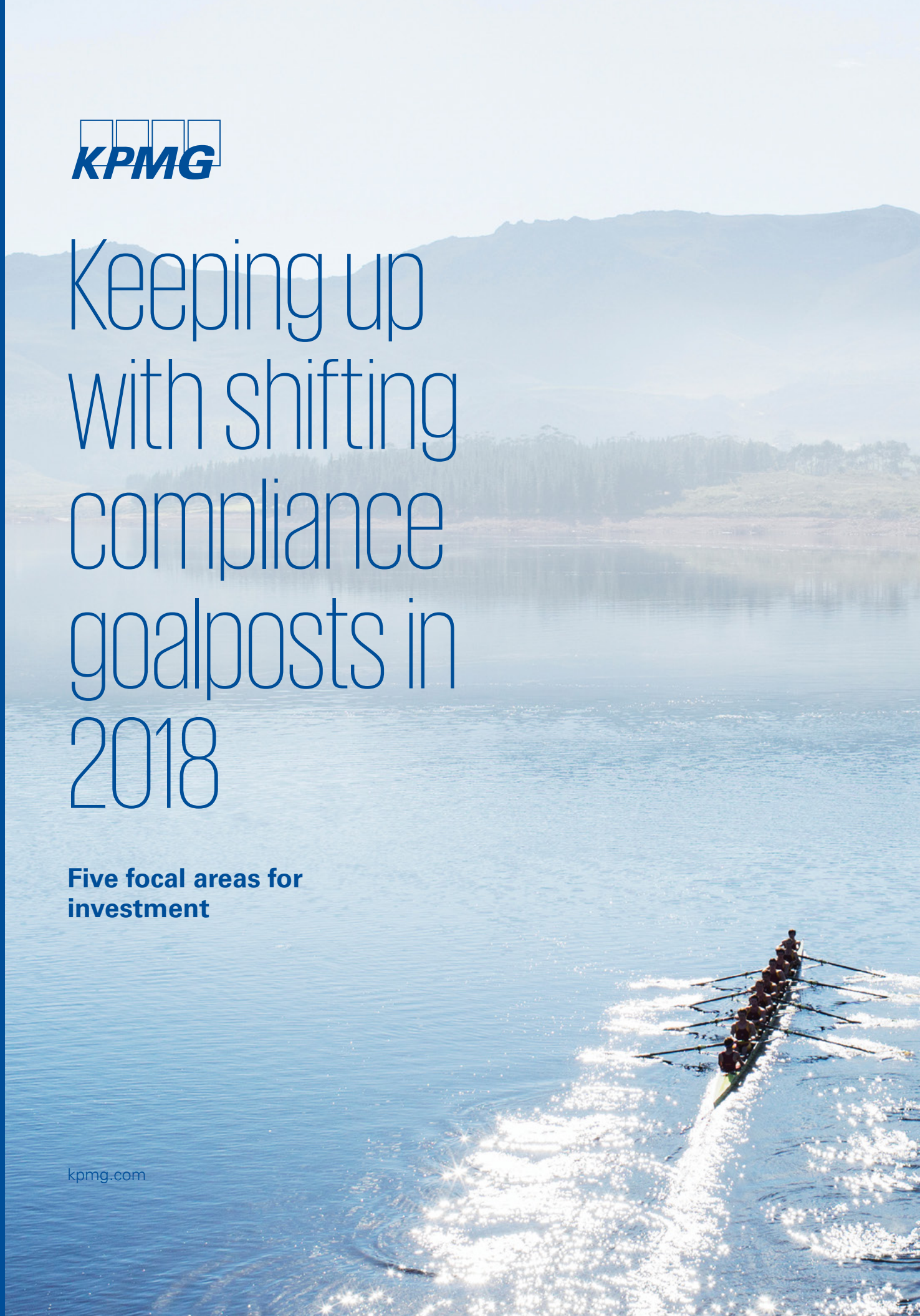


Keeping up with shifting compliance goalposts in 2018

Five focal areas for investment

kpmg.com

The need for agility and greater alignment between compliance and business strategy, coupled with continued refinement of regulatory requirements[1] and expectations, reinforce the need for organizations to continuously improve their compliance activities. By identifying and responding to shifts and trends in compliance early, compliance, business, risk, legal, technology and internal audit partners can better position their organization to move beyond compliance. In the future, integration and automation of compliance activities is an imperative. To prepare for tomorrow, organizations must invest today.

Investment in the following five areas can help you to better position your organization for the future:

1. **Operational integration** of the compliance program and minimization of silos, including with support functions such as Human Resources (HR), legal, finance, and other units in order to achieve greater coordination and consistency.

2. **Automation of compliance activities**, including to support regulatory change management, investigations, reporting (dashboards), testing and monitoring, and risk assessments.

3. **Accountability** of employees, contractors, and third parties to the organization's standards for compliance.

4. **Formalized risk assessments**, which need to inform further compliance enhancements and priorities, and should guide compliance officers in understanding compliance gaps for targeted mitigation.

5. **Continuous improvement of the program** through regular monitoring and root cause analysis.

We recognize that stakeholders across the organization are increasingly seeking greater compliance effectiveness, efficiency, cost cutting, and agility in compliance activities to further compete in the expanding digital and automated world.

Further integration and automation of specific compliance efforts can help meet these expectations, while also strengthening the organization's overall control environment, and the accountability of employees across all three lines of defense.

[1] This includes the Department of Justice (DOJ) Evaluation of Corporate Compliance Programs report, and in the financial industry the Office of the Comptroller of the Currency (OCC) through enforcement actions. In addition, other industry groups such as "Measuring Compliance Effectiveness: A Resource Guide" based upon the HCCA-OIG Compliance Effectiveness Roundtable Meeting, January 17, 2017, in Washington, DC.

KPMG

1. Operational integration

Regulators are increasingly spotlighting the need for operational integration within a compliance risk management program. Operational integration can be defined as integrating compliance into business processes and into people's performance of their job duties on a day-to-day basis. When compliance is operationalized, it is integrated in the organization's fabric.

An integrated compliance approach strengthens an organization's ability to understand and manage its risks, and to continuously improve and remediate trending issues. Integration improves the likelihood of an organization detecting a range of compliance issues—from fraud, sanctions, theft, or asset misappropriation to cybercrimes and corruption.

Key to operational integration is to include functions, such as HR, finance, legal, technology, procurement, and marketing, among others, in aspects of compliance management. Representatives from these functions should have a seat at the table as they each affect the compliance environment in unique ways, but often do not have traditional compliance roles and responsibilities. Their position allows them to offer information regarding gaps, weaknesses, or strengths in the compliance program, which can be relevant to evaluating its overall health and effectiveness. In addition, these functions should have clearly defined roles in supporting the compliance framework as well as in designing and implementing processes to facilitate the flow of data and information to the compliance function (and back to the functions). As operational integration develops, compliance leaders become more of a partner within the organization and greater coordination and collaboration occurs, enabling a more concerted and consistent approach to risk management.

Operational integration can also be enriched by mapping the organization's obligations inventory to enterprise-wide controls across operations, business units, and functions. This mapping helps to embed compliance in the daily lives of the employees, and to clarify their role in the compliance management framework.

Benefits of integration can include:

- Improved coordination and collaboration
- More thorough and holistic view of risks and trends
- Improved data aggregation and more thorough data analytic capabilities
- A more concerted approach to managing risks across the organization
- A common repository for data and a united technology infrastructure
- Heightened Board of Directors awareness and understanding of risks enterprise-wide
- A strengthened control environment
- Cost savings as a result of reductions in complexity and duplication
- Enhanced ability to comply with changes to an organization's regulatory expectations

Some organizations find that a more centralized governance approach or a hybrid approach to managing compliance efforts is best. By centralizing key compliance activities and processes at the enterprise-wide level, silos across the organization 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. In totality, this strengthens the organization's overall compliance risk management control environment.

In contrast, a decentralized approach to compliance presents certain challenges, especially as regulatory expectations around operational integration rise. With a decentralized approach, it can be hard to evaluate the extent to which compliance is operationalized, sustainable, and repeatable. There is also a risk that compliance approaches in some siloed units may not be as robust as needed to manage the risks. In addition, information that bears on the health and effectiveness of the compliance program may not be aggregated or unavailable, limiting the ability of compliance leaders, senior leadership, and the Board of Directors (Board) to understand and assess compliance risks and exposure across the enterprise.

Missed integration opportunity

A large financial institution had implemented a largely decentralized structure whereby its various business units had established compliance functions and HR departments that they controlled. These business unit functions collected metrics and data (e.g., termination rates, performance issues, investigations for wrongdoing) and then reported the results to the individual business unit leaders. However, the flow of information stalled at this level and was neither transparently escalated nor available outside the units from a centralized point of access, nor was the data able to be evaluated across business units which would have revealed a greater pervasiveness of the compliance risks, and shown that trends were not isolated.

A more integrated approach to compliance could have enabled compliance risks to have been detected sooner, and the severity of risks to be better understood by the Board. For example, the pervasiveness of the compliance issues could only be known from aggregated data across the enterprise. If this had occurred, it is more likely that trends would have shown the compliance issues and failures were a systemic issue, and enabled a root cause assessment, that with further investigation, would have mitigated the compliance issues and resulting customer harms.

KPMG

Role of support functions in the compliance control environment

Certain functions, including HR, procurement, and finance, are often independent of the lines of business but still implement processes that can impact the organization's overall control environment for compliance—supporting it when strong or exposing it to heightened risk when weak. For example:

The **procurement** function plays a major role, particularly in third-party risk management, and, from a compliance perspective, should support a control environment that manages third-party risks throughout the life cycle of the relationship.

The **legal** function tends to be responsible for activities such as complaint management, contract reviews, identification and management of legal obligations, and certain internal investigations, dependent upon the matter and severity. The legal function should support the organization's control environment for these activities and contribute reporting metrics that reflect on the health of the compliance program.

As the people management center of an organization, **HR** acts as a centralized aggregator of employee data, including employee complaints and investigation results, termination numbers, promotions, hires, and training. When viewed through a compliance lens, HR data can be quite telling about the health of the program, or indicate trouble areas for further focus and remediation.

With each of these functions, coordination and collaboration with the compliance function enables a more consistent control environment and hand-off of obligations and acknowledgement/management of identified risks.

2. Automation of compliance activities

Compliance leaders need to be actively engaged in determining how to implement technologies like machine learning to support their compliance activities. This is an imperative.

—**Andy Hinton**,
Chief Compliance Officer
Google

Compliance effectiveness increases when there is integration across an enterprise and successful automation of processes. Recent technological advances present a significant opportunity for compliance leaders to use technology and automate compliance activities while concurrently improving customer experiences. As compliance leaders are compelled to slim down compliance costs, and become nimble and more agile in an ever-increasingly competitive world, compliance leaders are responding by turning toward technology and automation (commonly referred to as intelligent automation[2]) that is applicable to their compliance activities and informed by the lessons learned in recent years from automating operational tasks. Currently, intelligent automation can be deployed to compliance activities such as: cybersecurity, monitoring and surveillance, regulatory change management, regulatory reporting, and, importantly, the development of predictive analytics.

Automation of these activities can enable the organization to further its risk coverage. Automating the reporting dashboards also enables better reporting to the Board and other senior leaders.

When adopting technology to automate compliance activities, it is important to remain alert to unintended risks that inevitably materialize, such as algorithmic biases, and insufficiently robust data. To help mitigate these risks, organizations can embed their risk and compliance frameworks up front in the design phase of their technology implementation, and then revisit its effectiveness continuously throughout the life cycle of their transformation and thereafter.

Important considerations when identifying compliance activities to support with intelligent automation include:

— **Compliance program goals for the future –** By starting at the finish line, and in consideration of their current state, compliance leaders can identify what steps will be needed to bridge the gap. This will translate into the needed resource inputs and related costs. In evaluating their goals, compliance leaders should consider what their organizations will need to look like across their people, processes, and technology in the future, so they can start building an appropriate infrastructure.

[2] Intelligent automation helps compliance leaders to respond to increased regulatory expectations while reducing compliance cost, increasing enterprise-wide coordination, and contributing to more agile business strategies. For further information as to how intelligent automation can be used in the financial services industry see, "The nexus between regulation and technology innovation," which can be found at https://advisory.kpmg.us/risk-consulting/frm/regulatory-ecosystem/reg-tech-innovation.html.

KPMG

— **Implementation dependencies and interdependencies –** Often there can be dependencies to automating processes and activities which should be considered and which may ultimately drive the ordering of automation that the organization will undertake. For example, if data integrity or accuracy needs to be improved before automation of a compliance activity can occur, this will need to be prioritized first. It is also important to assess existing and emerging technologies within an organization to determine functionality and any critical interdependencies across the three lines of defense that would be impactful.

— **How automation will support the business –** Tactical investments in the area of technology should have long-term benefits for both compliance and the profitability of the business. Compliance leaders should further coordinate and collaborate with the business when prioritizing automation initiatives.

— **Enhancing competitiveness and agility in executing its compliance activities –** As part of this assessment, compliance leaders should determine the strategic linkages between compliance program activities and available technology solution options for each activity. This often includes a comparison of potential technology vendors and analysis to determine whether to build, buy, or team with technology providers in automating specific compliance activities. 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. "Black box" solutions can pose risks and many vendors do not openly share their coding and methodologies, which can be a challenge to then validate for compliance assurance purposes.

Automating compliance activities can also help augment resource allocation, or allow for a resource shift to more strategic initiatives. For example, due diligence on third parties or day-to-day monitoring of transactions are repetitive tasks that machines increasingly can perform. Similarly, repetitive tasks exist in the testing arena and in regulatory change management. By allocating repetitive type tasks, and even some more cognitive tasks to machines, commonly referred to in this context as intelligent automation, compliance leaders can realize greater accuracy in core compliance functions.

Investing in technology and automation without a partnership with operations and a clear and grounded strategy from the C-suite can derail the journey and waste much-needed dollars. Business strategy must be an instrumental consideration in the design and implementation of a compliance risk mitigation strategy, which can then be embedded and supported by automation.

It is estimated that up to 45 percent of workplace activities can be automated. The benefits of digital labor (currently referred to as "intelligent automation") typically include higher efficiency and significant cost savings.[3]

[3] See KPMG's "Demystifying Digital Labor," 2016, available at http://www.kpmg-institutes.com/content/dam/kpmg/advisory-institute/pdf/2016/demistifying-digital-labor.pdf.

Integrating intelligent automation into compliance activities

Rapid innovations in technology are prompting many compliance leaders to embrace intelligent automation to support their compliance activities, achieve greater agility, and remain competitive.[4]

Intelligent automation can be utilized to support the following types of compliance activities:

Reporting and metrics – Collectively, reporting and metrics enable compliance leaders and other stakeholders to understand and evaluate their compliance risks and trends, particularly when aggregated across the organization. Cultural assessments and culture assessments are increasingly sought to substantiate the health of the compliance program and how well the culture is embedded. Technology and automation can be used to generate reporting dashboards that provide users with the necessary information (e.g., risk rating, trends) to monitor and improve their compliance program. Data quality rules engines can also be designed to support the assessment of "compliance" data for completeness, accuracy, quality, and integrity.

Compliance risk assessment – Risk assessments are central to an organization's continuous improvement in compliance and provide great insights into an organization's inherent risks, controls, and residual risks as well as risk trends. When compliance risk assessments have a consistent taxonomy and are automated, greater value is garnered and greater consistency in output can be realized, enhancing overall value from the investment. To the extent a compliance risk assessment utilizes quantifiable data and rubrics, scoring parameters or weighting, standardized templates and taxonomies, aspects of the process can be automated. In particular, automation can help with extracting data and information from documents that is required to support the assessment process and to feed various operational risk assessments and regulatory assessments into one overarching compliance risk assessment, and also then into a broader governance, risk, and compliance (GRC) assessment. It is noteworthy that valuable human analysis should also continue to be a component of the process.

[4] The term intelligent automation is used to refer to the spectrum of innovation that can be brought to bear on compliance efforts and activities today. Intelligent automation includes the use of robotics, machine learning, and the most sophisticated cognitive learning when a machine performs tasks otherwise performed by a human and learns from the experience.

KPMG

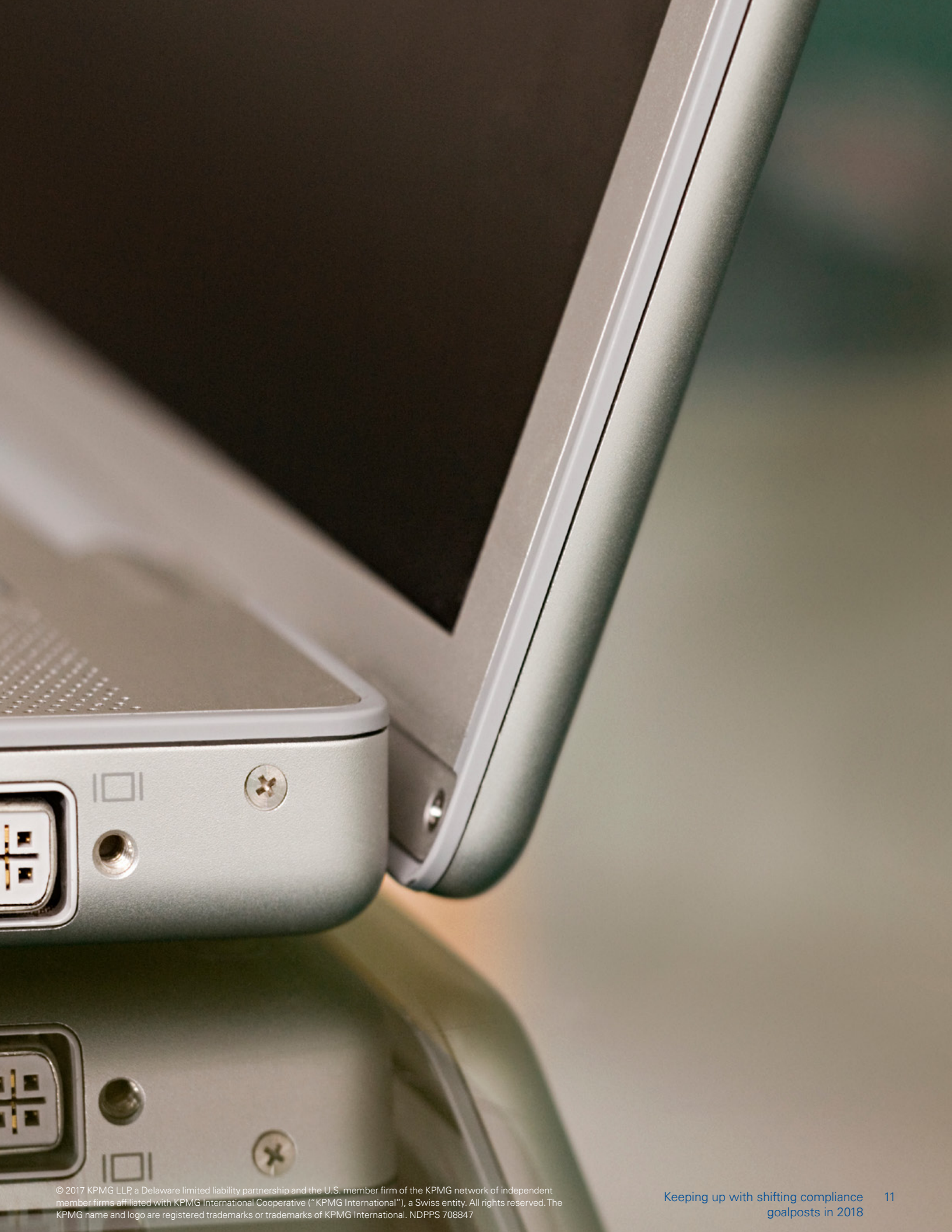
Inventory and mapping of regulatory obligations – A foundational aspect of compliance risk management is an awareness of the regulations that an organization must comply with and an evaluation of the associated risks. A comprehensive inventory of regulations that are mapped to an organization's policies, procedures, processes, and controls enables an organization to design and implement comprehensive coverage of its risks and adjust their compliance approach as new regulations, laws, and guidance are passed. A dynamic, automated approach helps to facilitate a timely response to regulatory changes that includes timely identification of risks, controls, policies, and procedures impacted by the regulatory change.

Data visualization and predictive analytics – Data visualization and predictive analytics help compliance leaders to view disparate data in an aggregated and holistic view. Techniques such as data mining and statistical modeling can be used to make predictions about unknown future events, enabling a more predictive approach to compliance risk management, and communicating information in an intuitive and informative way.

Monitoring and testing (across any of the three lines of defense) – Organizations have implemented compliance monitoring and testing efforts that vary greatly, often influenced strongly by their industry and existing regulatory obligations. Yet, compliance monitoring and testing is a key compliance activity that can be automated, helping organizations achieve greater risk coverage and consistency. For example, intelligent automation can be used to test more comprehensively across a population, thereby enhancing risk coverage with potential to test in real time. Automation can also be used to proactively identify risk trends and escalate failures across an organization.

Vendor and third-party oversight – Automation of third-party risk management activities enables organizations to better manage their compliance risks including by organizing their third-party relationship, providing more comprehensive knowledge of their relationships across the organization (when centralized), workflows and consistent assessment criteria, monitoring of vendor compliance with organizational requirements, and implementation of additional mitigating controls.

Issues management and investigations – Regulators are increasingly seeking to understand how organizations address their issues management and investigations activities, connectivity, and feedback loop to the rest of the compliance program and whether root cause analysis has been conducted fully. Automation assists organizations in managing their issues management and investigations activities comprehensively, tracking to complete, and with evaluation of issues/connectivity to other items.



3. Accountability

Organizations have to be willing to consistently make hard choices in order to demonstrate the importance of compliance and instill accountability in employees. Regulators increasingly expect organizations to implement performance management and compensation programs that encourage prudent risk-taking behaviors and business practices and emphasize the importance of compliance with laws and regulations.

Leading organizations are attuned to the need to work with HR to further embed compliance in their employee performance evaluation process. Often, this is incorporated as part of the "performance objectives" that are aligned with the organization's compliance strategy and risk tolerance. It also involves awarding bonuses and raises to those employees who are ambassadors of the compliance message, and disciplinary actions such as termination, decreases in compensation components, or warning letters for those who do not act in accordance with compliance requirements. Supervisors of a division where misconduct occurs may also be subject to disciplinary action on the basis that they neglected to provide sufficient oversight.

It is essential that disciplinary and incentive protocols be consistently applied to high-level employees. To do so sends a message that seniority and success do not exempt anyone from following the rules. In this sense, leadership must also hold itself accountable for lapses and failures. Failing this conveys the message to employees that compliance can be circumvented, or does not apply to everyone equally.

"You can have a sound compliance framework, and all the right policies and procedures in place, but if individuals who break the rules are not held accountable for their actions—especially if it is someone in a leadership position—the foundation of your program is compromised," stated Rich Girgenti, KPMG Principal.

KPMG CCO Survey

Our CCO Survey[5] identified that accountability is high on CCO priorities for enhancement. Specifically, 55% of CCOs identified "enhancing accountability and compliance responsibilities" as a top 3 priority in 2017.

39% of CCOs indicated that they do not, or do not know, if they factor employee compliance with policies and procedures into performance and compensation evaluations.

Only 29% of CCOs indicated that they conduct regular assessment of their team's compliance skills and proficiencies.

Some examples of "hard decisions" that organizations must be willing to make in order to instill a stronger sense of accountability among employees are listed below:

- Calling off a merger or acquisition transaction because leadership found that there was misconduct or unethical conduct underpinning the deal
- Terminating an individual in a leadership position for not acting in accordance with the organization's compliance policies or culture of compliance
- "Clawing back" an executive's compensation when it was earned based on fraudulent or unethical behavior
- Making enterprise-wide adjustments to the performance management system, including the incentive compensation structure to emphasize nonsales performance metrics or to eliminate/downplay sales goals and balance sales goals against employees' compliance.

[5] KPMG CCO Survey, https://advisory.kpmg.us/risk-consulting/compliance-transformation/kpmg-chief-compliance-officer-survey.html

KPMG

Additionally, regulators are starting to set clearly articulated expectations for how Boards can hold senior management accountable for executing an effective compliance risk management program as well as for day-to-day compliance efforts.[6] Some ways a Board can infuse such accountability in senior management include:

- Ongoing engagement of senior management in robust and active inquiries during meetings (inclusive of risk trends, drivers, and indicators)
- Allocation of sufficient time to Board meeting agenda items
- Individual evaluation of senior management individual's performance and compensation structure, as assessed against performance objectives, which are a mix of financial and nonfinancial
- Challenges to senior management's assessments and/or recommendations as warranted, including identification of gaps or weakness in the assessment
- Encouragement of diverse views.

> "Our risk and control programs are built on integrity. To create greater individual accountability for addressing ethical and other risk issues, this year compliance implemented integrity goals for our senior management and ORM implemented a "raise your hand" campaign."
>
> —**Karen Nelson, Chief Compliance Officer**
> AIG

Holding senior management accountable for compliance

Depending upon regulatory requirements, Boards should hold senior management accountable for:

- The quality and availability of information provided to the Board
- Timely remediation of the organization's internal testing results, or regulatory findings relevant to its compliance program, and other improvements to the compliance program
- Adherence to the Board-approved strategy and risk tolerance for relevant lines of business
- Material or persistent deficiencies in risk management and control practices
- Discerning which opportunities the organization should pursue or avoid, based upon the Board's risk strategy and established risk tolerances (based upon Board-articulated types and levels of risks)
- Determining the resources and controls needed to implement the Board's strategy

[6] See Federal Reserve Proposed Supervisory Guidance on supervisory expectations for Board of Directors, August 3, 2017, at https://www.federalreserve.gov/newsevents/pressreleases/bcreg20170803a.htm; also see Bloomberg's article, "Board Oversight of Risk and Compliance in a Changing Regulatory Environment," which can be found at https://advisory.kpmg.us/content/dam/kpmg-advisory/risk-consulting/pdfs/2017/07/bloomberg-bna-matsuo-girgenti.pdf.

4. Formalized risk assessments

Regulatory guidelines and expectations released in 2017 reinforce the need for compliance leaders to conduct compliance risk assessments on a regular basis. The DOJ Fraud-division Questions published in February 2017 set forth specific questions as to whether an organization has a "risk assessment," what methodology the organization employs in conducting their assessments, the information and analysis utilized as inputs in the risk assessment, and how the risk assessment captures "manifested" risks. As a result, regulatory expectations set forth specific focal areas that compliance leaders should ensure are covered in their assessments.

The DOJ's Questions reflect the critical role that compliance risk assessments have in a sound compliance risk management program. Organizations need to establish more sophisticated risk assessments to understand and assess existing compliance risk, evaluate risk trends, and anticipate future compliance risks that may manifest themselves in the future. Additionally, a compliance risk assessment should evaluate control environment gaps and weaknesses that senior management need to mitigate and provide visibility to as the highest compliance risks across the organization. Risk assessments also commonly serve as a road map for compliance leaders, informing the scope and frequency of compliance monitoring, testing, and internal audit test work, among other efforts. Leveraging the risk assessment also enables stakeholders across the three lines of defense to scrutinize higher risk areas and expand their risk coverage, and execute a more risk-based approach to compliance.

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

— **Proactive management of regulatory changes –** An inventory of compliance requirements, or obligations, helps organizations to understand the regulations that apply to their businesses, products, and services and across the jurisdictions where they operate. It is therefore foundational to the compliance risk assessment process and can aid in the identification of gaps and weaknesses in the control environment. To the extent organizations can implement a proactive and centralized approach to managing their regulatory change, they will be better positioned to respond to changes and better equipped to evaluate the impact on the organization of the change and the existing controls that may be leveraged or refined, or the new controls that are needed. Further, when organizations map their existing controls back to the applicable regulation(s), they can realize an additive benefit. This type of proactive and integrated approach to managing regulatory changes improves the organization's ability to assess gaps and weaknesses across its control environment, identify priorities for enhancement, and meet the goal of strategically managing the Board's risk tolerance.

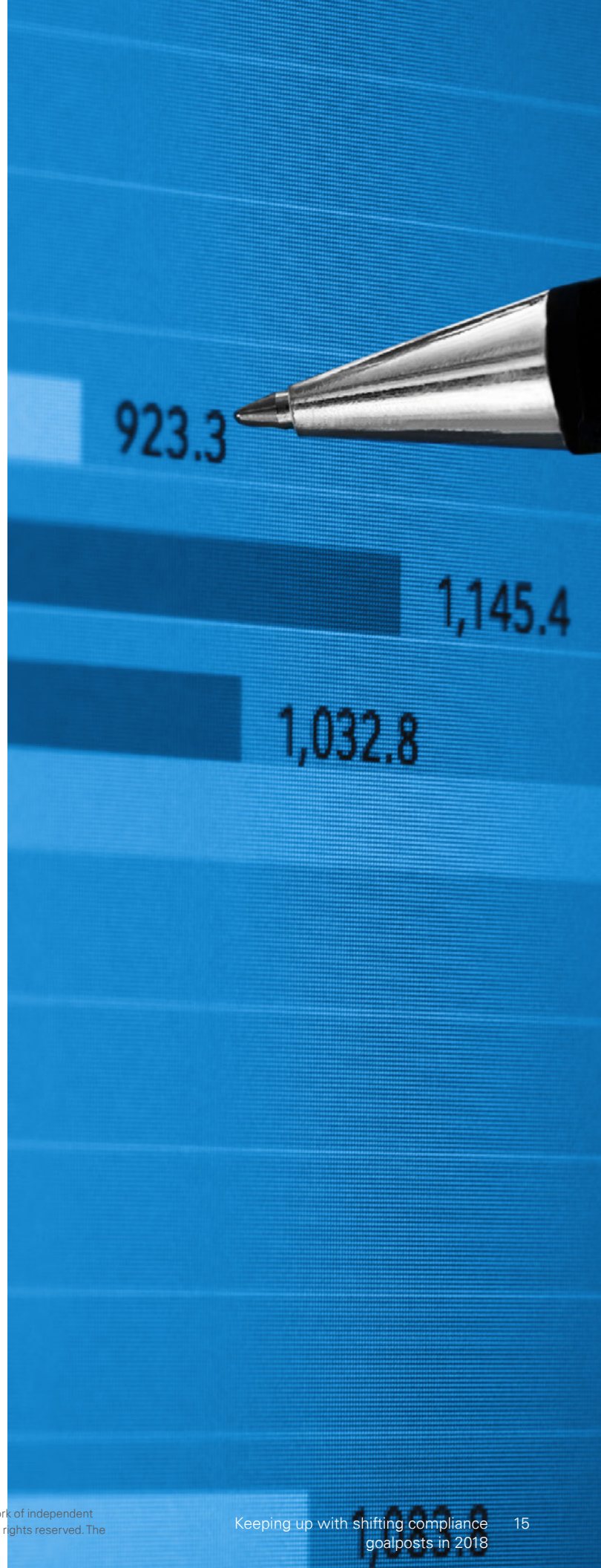
— **Refining the methodology –** As regulatory publications allude to, regulators are interested in understanding organizations' methodology for identifying, analyzing, and addressing their compliance risks. The value of a clearly documented methodology is well established. Importantly, it creates a blueprint for the execution of the compliance program that is sustainable and encourages a consistent implementation. For this reason, it is recommended that a risk assessment methodology set forth sufficient detail including how inherent risks, mitigating controls, and residual risks

KPMG CCO Survey

Our CCO Survey[4] identified that 24% of CCOs do not, or do not know, if their compliance risk assessment process considers whether internal controls are designed appropriately and operate effectively.

will be arrived at, and any formula to be applied. At the same time, the risk assessment should not be overly prescriptive. Further, given regulatory interest in understanding how metrics inform the overall compliance program approach as well as what metrics organizations collect and use, it appears particularly important that a risk assessment methodology outline the metrics the organization will utilize in its evaluation of compliance risks. In addition, if not already documented, compliance leaders should consider identifying the various roles and responsibilities of stakeholders in the methodology. Such stakeholders often include the Board, the compliance function, senior management, information technology and data scientists, business units and operational teams, and HR. A strong methodology also sets forth parameters for reporting risk assessment results to the Board in a digestible way, with guidelines for the level of data and information. This helps to ensure the Board is adequately informed with the right level of information to oversee the organization's risk management and tolerance.[7]

— **A feedback loop –** It is quite valuable to discuss final compliance risk assessment results with the 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 in the first line of defense. To the extent it exists, the feedback loop also provides business line leaders and compliance leaders with an opportunity to learn about differing views of identified risks and controls.



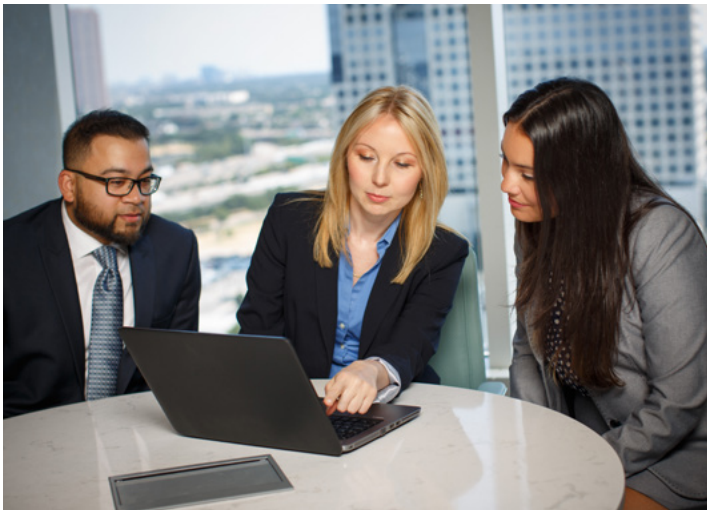
[7] For additional information, please see the December 2015 article in *Compliance and Ethics Professional* magazine titled, "Collecting and evaluating effective compliance program metrics."

5. Continuous improvement

Organizations need to continuously evolve their compliance efforts to ensure the control environment remains firm in the face of shifting regulatory expectations and requirements, risk trends, and emerging risks. Evolution is a necessity even when an organization's risk profile has remained virtually unchanged.

"Since the risk and regulatory environment is ever-changing, and innovative new technology is being developed at an unprecedented pace, compliance leaders need to consider how their approach to compliance should shift," Amy Matsuo, KPMG Principal, shared. To the extent that organizations have strong monitoring, testing, audit programs, and risk assessment processes, compliance leaders can utilize observations and findings from these efforts to inform program enhancements.

Monitoring, testing, auditing (hereinafter "testing") and investigations play a significant role in the compliance program life cycle and aid compliance leaders in identifying targeted ways to further minimize misconduct and continuously improve.



Regulators expect organizations to have a robust testing program, and in turn, for the results to be used in the "continuous improvement" of the program. Key considerations include:

- The type and scope of testing that the organization has completed
- Whether audits, in particular, have identified issues and findings
- If issues and findings have existed, how those items are reported to management and the Board, tracked, and remediated in order to mitigate the risks or plug control gaps
- Board follow-up on issues and findings, as applicable
- Whether audit's testing coverage is comprehensive and risk-based to identify potential misconduct with a particular focus on higher-risk issues
- The frequency of review of higher risk areas
- The extent of any control testing undertaken and any compliance data analysis

KPMG CCO Survey

Our CCO Survey[5] identified that 35% of CCOs do not, or do not know, if processes are in place to assess the impact of issues, root causes, and cross-organizational impacts and to create enterprise-wide solutions.

To continuously improve, compliance leaders ought to actively conduct ongoing evaluation of:

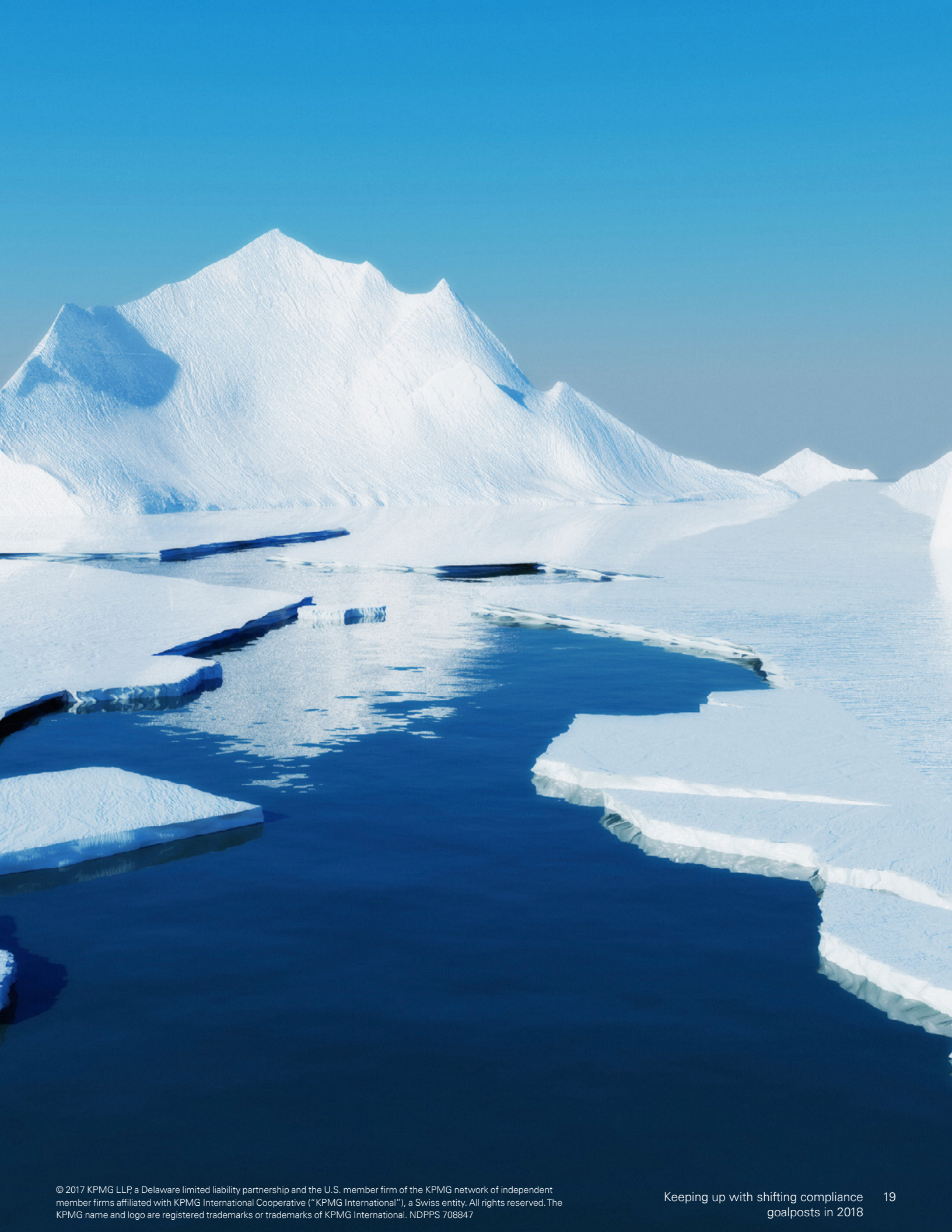
- Regular testing and audit efforts, including upon changes to the organization's risk profile (e.g., when introducing new products or services, changes to jurisdictional markets served, mergers or acquisitions, or relationships with third parties)
- Ongoing tracking of potential regulatory changes that have potential to impact the compliance program
- Market changes and trends that could impact compliance efforts and change the firm's risk profile, including with respect to technology
- Root cause analysis information and investigation outcomes
- Data that reflects the health of the compliance program, and missing or needed data that can support more predictive analytics
- Compliance gaps and tracking of remediation efforts.

Final thoughts

Compliance and business leaders must continuously improve their compliance activities in pursuit of greater effectiveness, efficiency, agility, and resiliency.

As market pressures encourage organizations to further cut costs, compliance and business leaders must continue to strategically invest in compliance activities that will expand their risk coverage, embed compliance enterprise-wide, and support business goals and objectives.

Compliance automation, operational integration, refinement of compliance risk assessments, and measures to reinforce accountability of employees, contractors, and third parties, are all ways to accomplish this. By continuously improving, organizations can methodically position their organizations for the future.



Contact us

Amy Matsuo
Principal, Advisory
Compliance Transformation (CT) Solution Global and National Leader
T: 919-380-1509
E: amatsuo@kpmg.com

Regina Cavaliere
Principal, Advisory
CT Healthcare and Life Sciences Co-lead
T: 973-912-5947
E: rcavaliere@kpmg.com

Dan Click
Managing Director, Advisory
CT Consumer, Retail, and Industrial Manufacturing Lead
T: 313-230-3240
E: dclick@kpmg.com

Carolyn Greathouse
Principal, Advisory
CT Technology, Media, and Telecommunications Lead
T: 314-244-4096
E: cgreathouse@kpmg.com

Stacey Guardino
Partner, Advisory
CT Insurance Lead
T: 212-954-4950
E: sguardino@kpmg.com

Julie Luecht
Principal, Advisory
CT Energy Lead
T: 713-319-3721
E: jluecht@kpmg.com

Anthony Monaco
Partner, Advisory
CT Government Lead
T: 212-872-6448
E: amonaco@kpmg.com

Todd Semanco
Partner, Advisory
CT Financial Services Lead
T: 412-232-1601
E: tsemanco@kpmg.com

Jennifer Shimek
Principal, Advisory
CT Healthcare and Life Sciences Co-lead
T: 973-912-6167
E: jshimek@kpmg.com

Acknowledgements: authored by Amy Matsuo, Julie Gerlach, and Nicole Stryker, with contributions from Jennifer Shimek, Hernando Garcia, Karen Staines, Todd Semanco, and Michael Lamberth.

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

kpmg.com/socialmedia