The compliance journey

Boosting the value of compliance in a changing regulatory climate

Summary of KPMG's CCO Survey results

2017

kpmg.com

Introduction

Compliance officers today face many challenges in their compliance journeys. The pace of regulatory change is swift. Regulatory requirements and expectations globally are constantly changing. New technologies and analytics are becoming increasingly important. In addition, there is continuing pressure to reduce costs and improve efficiencies at a time when the roles of the Compliance Officer are expanding beyond mere regulatory and legal compliance to include a wider range of concerns such as ethical standards and sustainability.

The many challenges in this current environment elevate the need for Chief Compliance Officers (CCOs) to develop a risk-based strategic vision for compliance. Such a vision is stronger when it is based on a robust understanding of the organization's current regulatory environment as well as the likely trajectory of regulatory change. The CCO can then utilize this information to prioritize core investment activities consistent with the compliance vision. Successful realization of the compliance vision will depend on the Board, senior management, executive leadership, and each of the three lines of defense sharing the same perspective and working toward the same goal.

To understand how organizations are responding to this changing environment, KPMG LLP (KPMG) surveyed CCOs from major organizations across seven industries regarding their compliance activities. KPMG's CCO Survey addressed the nine components in KPMG's proprietary Compliance Program Framework, including compliance risk assessment, governance and culture, technology and data analytics, and monitoring/testing, among others. By examining specific compliance activities across these nine program components, we believe the CCO Survey results can provide CCOs with vital information on how other organizations are managing compliance as well as highlight leading practices to consider implementing consistent with their organizations' risk profile and risk tolerance.

We trust that the CCO Survey results will provide you and your organization with valuable insights into additional program enhancements for you to consider.

Amy Matsuo
Principal, Advisory
Compliance Transformation
Solution Global and National Leader
919-380-1509
amatsuo@kpmg.com

Richard Girgenti
Principal, Advisory
Compliance Transformation
Solution Executive Sponsor
212-872-6953
rgirgenti@kpmg.com

Contents

Anticipated U.S. regulatory changes are creating uncertainty

In the wake of the U.S. elections on November 8, 2016, many expect the U.S. regulatory environment to undergo substantive shifts and changes, with the greatest impact on highly regulated sectors such as healthcare, life sciences, energy, and financial services. In the final days of the Obama administration, 140 "midnight" regulations were passed, which will impact compliance obligations for the financial services and pharmaceutical industries as well as establish environmental requirements for certain organizations.[1] In contrast, the new administration campaigned on a theme of lesser regulation, including references to overhauling, if not completely dismantling, certain areas of regulation around Dodd-Frank and the Affordable Care Act. During President Trump's initial days in office, the new administration has quickly begun to implement many such changes.

For many CCOs looking to enhance their compliance programs, this regulatory uncertainty can make it challenging to identify where to prioritize their compliance efforts.

Yet many of the CCOs we speak to recognize the need to "stay the course" in this time of uncertainty. It is important to remember that while changes to specific regulations are anticipated and are already occurring, compliance is broader than any one regulation. Further, the tenets of good risk governance, conduct, and culture are already entrenched in the expectations of regulators and consumers globally.[2] Additionally, global regulatory trends support better corporate governance and risk management, not reversals of it. Therefore, CCOs' overall commitment to instilling and enhancing a culture of compliance within their organization and their vision for further strengthening governance, compliance, and risk management as part of their risk-based strategy should continue to guide them forward despite this time of uncertainty.

It will likely take time for the new administration's agenda to come to fruition and for the impact of the Obama administration's "midnight" regulations to be realized. A continued focus on the larger compliance picture and emphasis on how to enhance one's effectiveness, efficiency, and agility through tactical efforts remains a strong course of action for CCOs.

1 Source: *Washington Times*, News section, January 5, 2017.

2 Source: Compliance Week, Compliance Officers Scratch Heads as U.S. Trumps Brexit, Paul Hodgson, November 22, 2016, noting that organizations have invested a huge amount of time and money putting in place controls and control mechanisms, and it is difficult to imagine that just removing legislation will immediately affect organizations' culture.

Executive summary

KPMG's CCO Survey found that organizations across seven industries[3] are making substantial progress in their compliance journeys, particularly in refining the foundational areas of their program such as **governance and culture, policies and procedures,** and **communication and training.**

However, organizations can make more progress in their compliance activities by further integrating processes and controls to detect and respond to potential misconduct such as **monitoring and testing** efforts and leveraging the power of **technology and data analytics**. In addition, most organizations recognize they have much more work to do to in the area of **people, skills, and due diligence**, especially when it comes to third-party due diligence processes, assessment of employee compliance skills, and fostering greater accountability for compliance across all three lines of defense.

KPMG's CCO Survey examined the specific approaches to compliance that CCOs are taking in each of nine core compliance components, depicted in KPMG's Compliance Program Framework. These components encompass the range of compliance activities that CCOs typically concentrate on when assessing the effectiveness of their compliance programs and setting priorities for improvement.

KPMG's Compliance Program Framework

Strongest program components

Across the nine compliance components, organizations generally report having strong programs in three primary areas that are "preventive" activities: **governance and culture, policies and procedures,** and **communication and training**.

— **Governance and culture**: In the area of **governance and culture**, most CCOs report that the board of directors (Board) or a committee of the Board annually reviews and approves the compliance program and also receives reports on how the organization is mitigating compliance risk. In addition, most organizations have a code of conduct that clearly communicates expectations to employees regarding the compliance culture. Yet many CCOs recognize that their lines of business could take greater ownership of the organization's compliance culture and agenda and do not perceive that employees recognize the competitive advantage provided by a strong compliance culture and good conduct.

— **Policies and procedures**: Most respondents also have implemented **policies and procedures** to support their compliance programs. These policies and procedures generally align with the organization's mission, vision, and values. In addition, most organizations have documented compliance requirements in their code of conduct and related compliance policies and procedures. Furthermore, many CCOs report that they have a formal process and personnel tasked with managing updates to their compliance policies and procedures. Yet, many organizations could still improve their processes for incorporating relevant changes in laws, rules, and regulations into their documented compliance programs.

3 KPMG's CCO Survey participants operate in the following seven industries—financial services; insurance; energy; healthcare and life sciences; technology, media and telecommunications; consumer markets; industrial manufacturing.

— **Communication and training**: This is another area of strength for many organizations, with most CCOs reporting that they have implemented comprehensive compliance training programs for all employees, inclusive of training on internal policies and procedures, and that new employees receive compliance training appropriate to their roles and responsibilities. Training of third parties, however, remains an area where additional improvements are generally needed, with many organizations not having a formal annual training program for their vendors. In addition, some CCOs could further incorporate communication strategies to share compliance issues, best practices, and lessons learned across the organization.

Program components needing greatest improvement

The survey also identified three areas where substantial improvements in compliance programs could still be valuable: **technology and data analytics; monitoring and testing;** and **people, skills, and due diligence** (including third-party due diligence). It is noteworthy that both **technology and data analytics** and **monitoring and testing** are "detective" activities in KPMG's Compliance Program Framework. As organizations develop more mature compliance programs, they work to strengthen the preventive elements of their programs and further develop capabilities to detect potential future problems. The Survey results suggest that, especially for these three components, many organizations could still make substantial progress in their journey towards more robust compliance programs.

— **Technology and data analytics**: Across the nine compliance components, organizations report the least progress with respect to **technology and data analytics**. Many organizations say they do not know or do not leverage technology to support their compliance initiatives. In fact, more than half of respondents do not, or do not know if they use Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs) in support of their monitoring and testing or to drive root cause analysis and trend reporting. Further, they do not integrate KRIs/KPIs into compliance governance and risk management efforts. Most CCOs have not, or do not know if they have, confirmed that their technology infrastructure aligns with their compliance requirements and whether any significant gaps have been addressed. Most organizations also do not utilize, or do not know if they utilize, an enterprise-wide tool with KRI/KPI monitoring capabilities for their third-party risk management.

— **Monitoring and testing**: Most CCOs report that they undertake periodic compliance program assessments to confirm that their program aligns with changes in the regulatory environment and with the expectations of key stakeholders. They also typically report testing results to management with tracking of open items (due dates and status), and many summarily report to senior management and a committee of the Board as well. However, a significant portion do **not** have a compliance **monitoring and testing** program that encompasses process, control, and transaction testing or that monitors and tracks regulatory change. Many organizations also struggle to monitor their third-party vendors, often lacking a process, or are unaware if their vendors have a process, to confirm they adhere to compliance due diligence processes and are not aware of utilizing technology to manage third-party risks.

— **People, skills, and due diligence**: While most organizations address compliance infractions in a timely manner and have established onboarding due diligence standards (for third parties and employees), in many other respects CCOs can do more to instill accountability across their organizations. For example, many respondents reported they do not assess compliance skills annually for their first-line and second-line personnel, and a significant number of CCOs do not have (or do not know if they have) defined compliance roles and responsibilities for their first-line and second-line compliance personnel, and do not consider adherence to compliance policies and procedures as a factor in performance ratings and compensation decisions.

"To advance your compliance effectiveness, efficiency, and sustainability, it is essential to execute not only against a sound compliance framework but to continue to invest in compliance regulatory automation. Through compliance investment (versus simply "compliance cost"), you drive not only enhanced compliance integration to the compliance risks in your business practices and control environment, but the ability to further expand your compliance predictive analysis."

– Amy Matsuo, KPMG Principal, Advisory; Compliance Transformation Solution Leader

Key findings

Board of directors provide active oversight. More than **90%** of CCOs report their Board or a committee of the Board is adequately informed of compliance risks and mitigation efforts. The group meets annually to review and approve the compliance program.

More involvement needed from lines of business. 36% of CCOs do not know, or disagree, that their lines of business management take ownership of the compliance culture and agenda. Only **15%** of CCOs strongly agree with this statement, indicating that for many organizations room exists for growth.

Communicating to employees the importance of compliance. 31% of CCOs do not know, or do not communicate, conduct and culture lessons across their organizations. Further, **29%** of CCOs have not documented, or do not know if they have, formalized compliance roles and responsibilities for their staff—it is foundational for employees to understand the importance of compliance and their role within the compliance structure.

Desire to instill greater compliance accountability. While CCOs report that they address compliance infractions in a timely manner and with appropriate disciplinary actions, almost 4 in 10 CCOs (**39%**) do not consider (or do not know if their organization considers) employee adherence to compliance policies and procedures as a factor in performance ratings and compensation decisions.

Regular skill assessments of staff is not a widely adopted practice. Only **29%** of organizations report that they assess compliance proficiencies and skills of their staff on an ongoing basis.

Compliance policies and procedures almost universal. At least **94%** of organizations report that compliance requirements are embedded within their policies and procedures and separately also within their code of conduct, which is accessible to all employees.

Keeping pace with regulatory changes. Only **27%** of CCOs strongly agree that the compliance function has a change management process in place to identify and incorporate changes in laws and regulations and to incorporate such changes into their policies and procedures.

Potential to enhance the compliance risk assessment process. While **84%** of CCOs report having a compliance risk assessment process that leverages qualitative and quantitative measurements, **32%** do not agree or do not know if their business unit, operations, and IT management are involved in assessing compliance risk within their units. In addition, roughly one-third of CCOs do not (or do not know if they) conduct reassessments of their risk profiles upon business changes.

Opportunities to leverage technology. Only **69%** of CCOs say their organization leverages technology to support its compliance initiatives, while less than half—just **47%**—say they use data analytics and other technology processes to conduct root cause and trending analysis.

Many organizations could implement more robust compliance testing. 33% of CCOs report they do not have, or do not know if their compliance testing program includes transactional, process, and controls testing, and only **27%** of CCOs strongly agree that they monitor and track for regulatory changes.

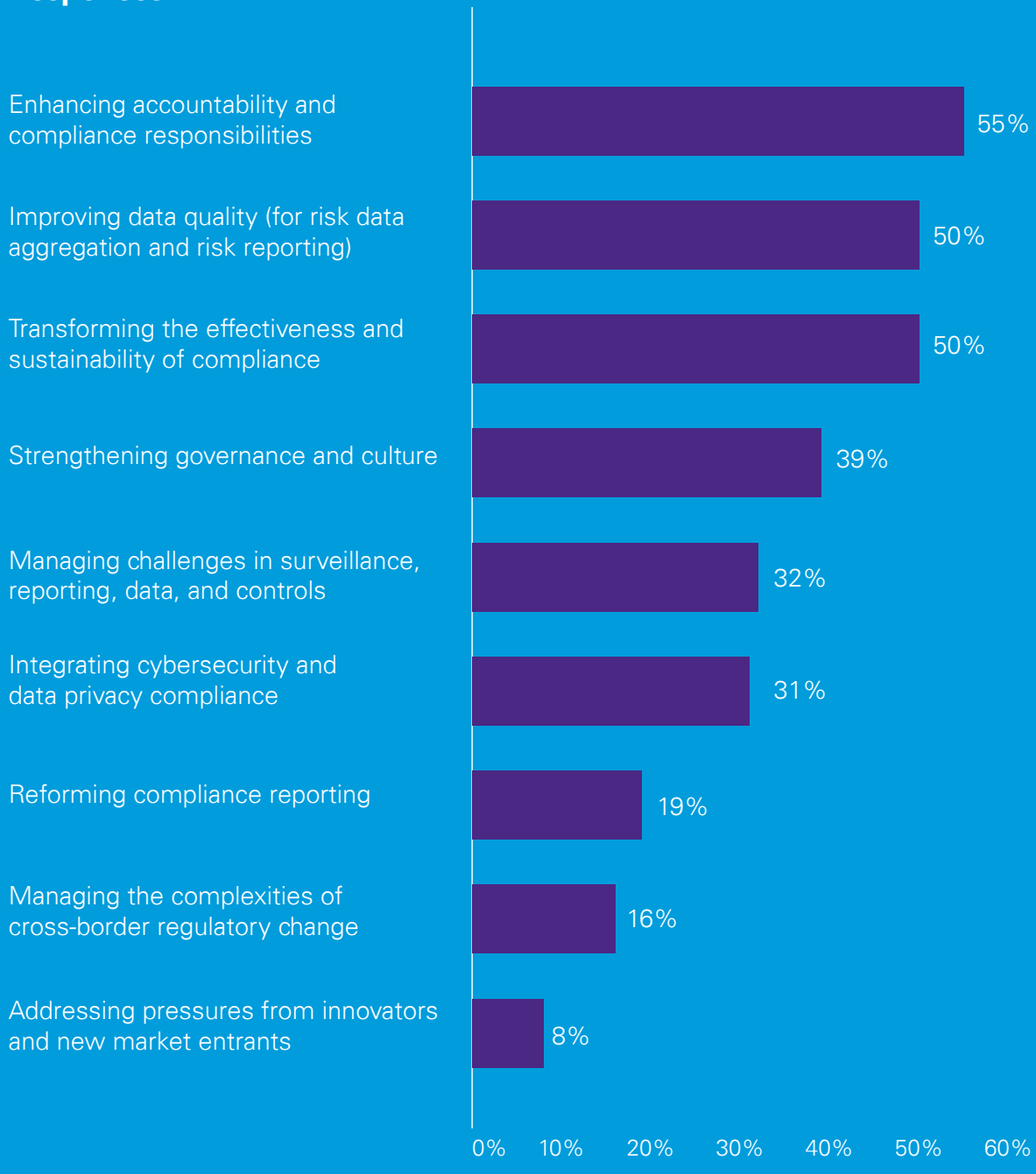
Widespread use of enterprise-wide compliance reporting. 84% of organizations provide reports on the enterprise-wide state of compliance including culture, conduct, governance, and key issues. Yet, only **47%** of CCOs say their organization has an enterprise-wide reporting system that is integrated with compliance monitoring and across functions and business units.

More monitoring of third parties can occur. Slightly more than **half** of organizations have a compliance monitoring process to confirm that third-party vendors adhere to compliance due diligence processes, and just **31%** manage third-party risk and issue tracking through an enterprise-wide tool capable of monitoring KRIs/KPIs.

Top compliance challenges[4]

When asked about their top compliance challenges, respondents each identified up to three of the following:

Responses



4 CCOs could select up to three answers, so percentages aggregate to over 100%.

The three lines of defense model

By: Julie Gerlach, KPMG Managing Director, Advisory

An effective compliance infrastructure enables strong governance, robust risk identification and mitigation processes and accountability, along with a culture of compliance across all three lines of defense. The three lines of defense structure provides for allocated compliance responsibilities across the organization defining who will own and manage risk, regardless of the size and complexity of an organization. The roles and responsibilities across the three lines of defense are typically established as follows:

- The **first line of defense** (line of business management and operations) typically owns and manages risks and controls. It identifies key risks to the organization and implements ongoing processes, systems, and programs against defined standards that build and support a culture of integrity.
- The **second line of defense** (compliance function) monitors compliance risks and controls in support of management. The compliance function is responsible for driving the overall design and implementation of the organization's compliance function, advising management and the Board, and assessing the effectiveness of the organizations control environment to help ensure that the business is designing and implementing effective controls intended to mitigate risks.
- The **third line of defense** (Internal Audit function) provides assurance on the effectiveness of controls in place to mitigate risk.

Although neither senior management nor the Board is considered to be part of one of the three lines, these parties collectively have responsibilities for establishing an organization's objectives, defining high-level strategies to achieve those objectives and establishing governance structures to better manage risk. Their engagement is critical for the success of the overall model and compliance program.[5]

One challenge many CCOs face is how to further instill ownership in the first line of defense so that the business units "own" their compliance risks, monitor their risks, and asses their controls for risk mitigation. One means of doing so is to establish formalized documented roles and responsibilities for each line with respect to management of compliance risks as well as for specific employees. This helps to ensure a consistent understanding of the role each line plays in the control framework. In addition, this exercise can provide a valuable opportunity for all stakeholders to review the responsibilities, identify if there are any gaps in control assessments across the organization, and even reduce duplication in test work. Ongoing communication and coordination is also particularly important and valuable for the three lines of defense model to be effective and functional.

"Everything is technically compliance, so it is essential for organizations to define the risk universe of compliance and what compliance should be doing and monitoring."

– Greg Catron, CCO, Humana

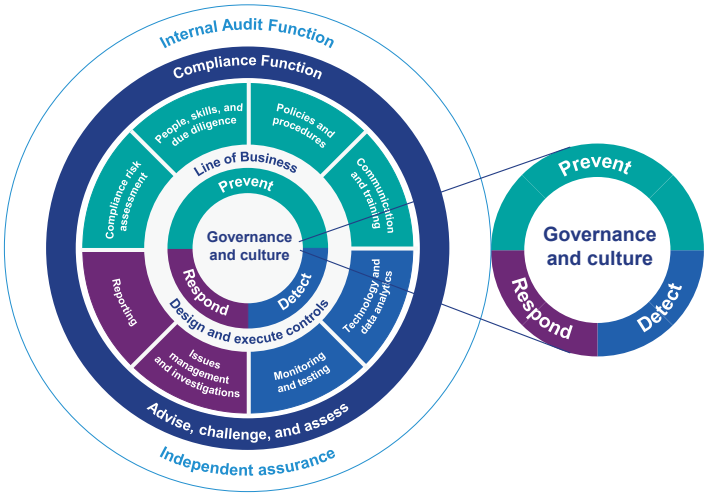
5 Source: Institute of Internal Auditors. Leveraging COSO Across the Three Lines of Defense. http://www.coso.org/documents/COSO-2015-3LOD-PDF.pdf: n.p., 2015. Page 1.

II Governance and culture

Governance and culture are the foundations of an effective compliance program. Governance commonly refers to a structure of compliance across the organization, while compliance culture is a combination of customs and beliefs about compliance within the organization. Embedding culture, or changing it, requires a formidable effort. But given how fundamental these two concepts are to a compliance program, it is no surprise that in KPMG's CCO Survey an estimated **39%** of CCOs identified strengthening their governance and culture as a top compliance challenge. This is also consistent with KPMG's client experiences, which reflect that, increasingly, Boards are enhancing their focus on effective governance and proactive risk management.

While many organizations have an active Board, established Board committees, and an involved and engaged CCO, the mandates could be more robust to incorporate and address changes in the regulatory environment that impact the organizations. For example, **82%** of CCOs report that they participate in enterprise-wide governance committees and interpret and provide guidance on KPIs related to compliance. Further, **almost all** organizations reported that their Board and/or delegated Board committee annually reviews and approves the compliance program (**94%**) and is adequately informed of compliance risks and how the organization is mitigating them (**93%**). Yet, when it comes to regulatory change, governance slips. Here, **22%** of CCOs reported that they do not know or do not have Board or delegated committee process in place to review the compliance management program upon changes in the regulatory environment based on a strategic assessment of enterprise-wide initiatives.

KPMG's CCO Survey also reflects the great progress many survey respondents have made here as well as areas for continued improvement to further embed a "culture of compliance" enterprise-wide. A culture of compliance is present when employees understand the value the organization places on integrity, trust, and respect for the law. To infuse a culture of compliance across the



organization, the Board and senior management need to set a "tone at the top and mood in the middle" that communicate the importance of compliance and ethical conduct. Beyond simply communicating these values through words, the Board and senior management must be seen to act in accordance with them. Regulators are increasingly focusing on whether organizations have a strong compliance culture, which is seen as an overarching control against misconduct.

Most CCOs agree that employees understand the culture and expectations for good conduct and ethical behavior (**87%**) and many believe their employees also see good culture and conduct as a competitive advantage (**68%**).

However, **36% or one-third** of CCOs disagree or do not know if line-of-business management takes ownership of the organization's compliance culture and agenda. In addition, **31%** of CCOs do not agree or do not know if lessons learned regarding conduct and culture are communicated throughout their organization. When lessons learned are not communicated throughout the organization, this is truly a missed opportunity, and significant value is left on the table. Communicating with employees when events occur (internally or

externally) or trends are identified can be a prime time to remind employees of their compliance responsibilities. For example, the recent fraud in the financial services sector can be a lesson to employees across all industries about the importance of a compliance culture, the need for every employee to act ethically, and for the desired behavior to be modeled by employees at every level of management. Similarly, lessons learned from an internal investigation, as well as lessons learned outside the company, can provide an opportunity to remind employees of their compliance responsibilities with respect to specific laws, regulations, or activities.

Including real-life stories and dilemmas in these communications, particularly communications from senior level management, can be quite impactful particularly in short video vignettes (with trackable "hits"). Supported by compliance training and other types of compliance activities, a refined communications approach can help to enhance and further embed a compliance culture. Furthermore, establishing an open atmosphere where employees feel free to report potential compliance or ethical problems and are encouraged to provide input about the organization's activities is key.

CCOs agree:

Annual review and approval of compliance programs by Board or committee — 94%

The Board is informed of compliance risks and mitigation efforts — 93%

Compliance Officers are involved in governance efforts (committees and KPI communications) — 82%

However, areas for growth include the following where at least 30% of respondents disagreed or do not know if:

Employees understand a strong culture and good conduct as a competitive advantage — 32%

The business unit management "owns" compliance culture and agenda — 36%

Conduct and culture lessons are communicated — 31%

Embracing a culture of compliance

By: Deborah Bailey, KPMG Managing Director, Advisory; and Tim Hedley, KPMG Partner, Advisory

Culture is the intangible that is reflected in the choices and behaviors, or conduct, of a firm's employees. It has been described as "the implicit norms that guide behavior in the absence of regulations or compliance rules—and sometimes despite those explicit restraints."[6] In the past year alone, compliance culture has been cited in regulatory actions across industries and in scandals as a root cause of misconduct, highlighting the continued need for a "good" corporate culture. Oftentimes, regulators have identified situations where a compliance culture does not exist and decisions are not supported by effective challenge, allowing misconduct to continue without escalation or without proper attention by senior management. As a result, many CCOs are questioning how can they ensure their compliance program is more than just a paper program, and how can they continuously reinforce their culture with employees.

A focus on the following compliance features within your organization can help you to further assess your compliance culture:

- The extent to which the first line of defense is educated about compliance
- How prevalent "effective challenge" is within the organization and whether there are any pockets where it is deficient or does not exist
- How the organizational strategy and direction (as well as business objectives) are influencing conduct and culture and how the organization's business objectives work in furtherance of compliance activities
- The organization's incentives and disciplinary protocols and how these protocols align with the organization's desired culture (such as promotions, pay incentives, etc.)
- The presence of subcultures that can impair the organization's cultural values
- How the organization is reinforcing its culture on a day-to-day basis[7]
- The approach and tools used by senior leadership, including management and executives within the business units, to consistently reinforce the message of compliance
- The processes and actions of the organization and whether these are in line with the organization's values, ethics, risk appetite, and policies.

Additionally, it is important to remember that:

- Culture cannot be imposed. Leaders must be role models, but ***culture must be shaped and enacted at all levels***—the voices of line management and middle management are key. Each individual is a "cultural carrier."
- Culture is experienced most intensely when there is a dilemma between conflicting objectives. These are called ***"moments of truth"*** and are useful starting points to examine culture and can serve as the basis for scenario-based learning.
- Culture needs to be ***constantly reinforced at a conscious and subconscious level***. Potent symbols, personal narratives, and subtle behavioral nudges are the psychological language of culture.
- When compliance can be overridden by the business, and improper conduct exists without accountability, the compliance function may be rendered ineffective.

6 Source: KPMG, Approaching the Crossroads of Conduct and Culture, Deborah Bailey, 2016.

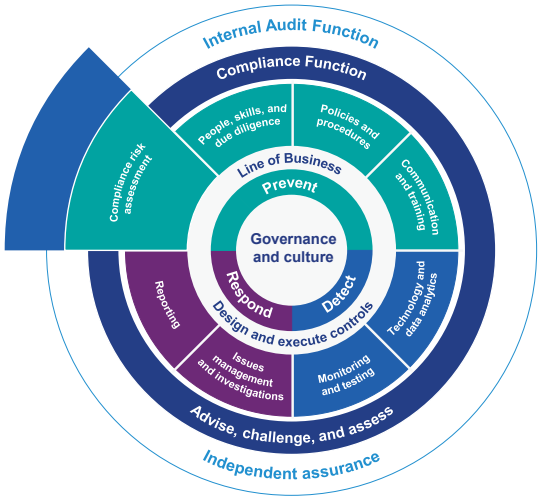
7 Amid a recent fraud in the financial industry, an organization's Board stated it would "take all appropriate actions to reinforce the right culture and ensure that lessons are learned, misconduct is addressed, and systems and processes are improved." In the same article, the other peer institutions' CEOs are also quoted as calling for a "culture of integrity" and needing to "redouble" efforts to reform their compliance culture after making "a number of mistakes – some of them quite painful and costly – over the last several years," for their respective institutions. Source: Wells Fargo scandal reignites debate about big bank culture, Gran, Olivia, Reuters, September 28, 2016 at http://www.reuters.com/article/us-wells-fargo-accounts-culture-analysis-idUSKCN11Y1S1.

Risk assessment

Organizations should periodically assess their risk of criminal conduct and shall take appropriate steps to design, implement, or modify their compliance program to reduce the potential risks identified. While most U.S. organizations recognize how fundamental an assessment of risks is to their compliance program approach, organizations vary significantly in the standards established for conducting risk assessments, the level of analysis conducted and documented, and how they involve first line of defense personnel in the process.

In KPMG's CCO Survey, **79%** of organizations report that they have a compliance risk assessment process that considers compliance risks across multiple jurisdictions inclusive of products and services. Even more respondents—**90%** of CCOs—report that their organizations identify, assess, and categorize inherent compliance risks. However, at least **23%** of CCOs do not consider as part of their risk assessments (or do not know) whether internal controls were designed appropriately and are operating effectively to mitigate risks nor do they determine and assess residual compliance risk across their enterprises. Survey respondents also differ in the use of qualitative and quantitative inputs to their risk assessments, with **84%** of CCOs stating that their risk assessment leverages both, although this is significantly lower for consumer market organizations (only **38%**). Further, KPMG's CCO Survey also found that many organizations have more work to do in fully involving their business units and functions in the assessment of compliance risk. Specifically, **32%** of CCOs do not agree or do not know if management in business units, operations, and IT are involved in the assessment of compliance risk within their units.

While compliance officers in more heavily regulated sectors tend to complete an inventory of their regulatory obligations as part of their risk assessment process, across other industries this is not implemented to the same degree. Specifically, while **77%** of all respondents report that they maintain a regulatory obligations inventory, within the consumer markets sectors only **50%** of organizations do, and within healthcare and life sciences only **54%** reported they do. This is likely correlated to regulatory expectations, yet it is clearly a better practice worthy of consideration.



Furthermore, for global organizations, which must comply with a myriad of regulatory obligations that differ country to country, a formalized inventory of their regulations should be the foundation of their compliance programs, and in an ever-changing world, this process should capture regulatory changes and trends. Without an inventory of regulatory obligations, CCOs are challenged to fully understand what compliance risks they have (stemming from each regulation) and to assess whether existing controls are sufficient to mitigate those risks. Uncontrolled risks could be present in the "black hole" of uninventoried regulations.

In addition, CCOs outside of the financial services sector appear to struggle with ongoing reassessments of their risk profiles due to business changes and do not have a dynamic and sustainable process in place. For example, while **85%** of financial services CCOs have a governance committee including representation from the compliance function that reviews changes in the organization's geographic footprint, and new products and services for compliance implications, this is not a widely adapted practice in other sectors. Only **38%** of consumer markets organizations and only **40%** of industrial manufacturing organizations have implemented such a practice.

Risk assessment (continued)

CCOs agree:

Their risk assessments include identifying, assessing, and categorizing inherent risks — 90%

They have a formal compliance risk assessment process in place — 79%

They incorporate qualitative and quantitative inputs (although this varies by industry, and some industries report significantly lower agreement than others) — 84%

The areas for growth in risk assessments include those areas where 20% or more of CCOs disagreed or do not know if their organizations' risk assessment processes:

Consider whether internal controls are designed appropriately and operate effectively — 24%

Include an assessment of residual risk — 23%

Involve first-line supervisors in the risk assessment process — 32%

Include an inventory of their regulatory obligations (though more CCOs in healthcare/life sciences and consumer markets disagreed or do not know) — 23%

Includes reassessment of their risk profile by a governance committee upon business changes (other than financial services) — 40%

Assessing compliance risks

Q&A with Stacey Guardino, KPMG Partner, Advisory; Compliance Transformation industry lead for insurance

Slightly less than **80%** of CCOs report in KPMG's CCO Survey that they have a formal compliance risk assessment process in place, and **90%** of CCOs identify, assess, and categorize inherent compliance risks. However, further opportunities for enhancement exist. **Stacey Guardino**, Compliance Transformation industry lead for insurance offers her perspective on the opportunities that exist for organizations to further enhance their compliance risk assessment approaches.

What are better practices you have observed for assessing compliance risks?

We see many clients that assess their inherent risks by considering the probability and the impact of compliance risks by product/service, line of business, legal entity, and/or country supported by an underlying inventory of legal/regulatory obligations. For many, the inherent compliance risk assessment is largely qualitative; however, some leading organizations are able to obtain internal quantitative data to support their inherent compliance risk assessments, which can make the assessment more valuable. For example, when considering anti-bribery and corruption (ABC) compliance risk, the organization may rely upon data that quantifies the number of third parties it does business with, their risk ratings (if such exists), the location of those partners, the length of relationships, and other risk factors. This type of information helps to quantify the ABC compliance risks across the organization for the Board and other stakeholders.

Once the compliance function has a good grasp on the organization's inherent compliance risks, it is very important that they understand the key internal controls (both preventive and detective controls) the organization has implemented to mitigate the compliance risks. For example, these controls may include policies and procedures, training, ongoing communications, and automated controls. Mature organizations should have a well-documented compliance risk assessment methodology, including descriptions of how residual risks are determined (inherent compliance risk minus internal control effectiveness rating equals residual compliance risk). Some organizations apply formulas and weightings to qualitative data to convert it to quantitative measures and also utilize heat maps to report compliance risk assessment results. Approximately 20 to 25% of CCOs responding to KPMG's CCO Survey indicated that they do not know, or do not currently assess their internal controls and residual compliance risks so these organizations have an opportunity to enhance their compliance risk assessment processes.

Additional better practices that we see include:

- Identification and assessment of emerging compliance risks/trends and changes year over year
- Involvement of business units, operations, and information technology in the compliance risk assessment process, including establishing a feedback loop. This helps the first line of defense to be accountable for their compliance risks as they own their assessment process and receive feedback on it from the second line
- A consistent compliance risk assessment methodology utilized across the organization, which enables the aggregation of information such as the risk rating criteria utilized, the detail and level of granularity in each assessment, the taxonomy (definitions) used to describe different compliance risks and internal controls, and, to the extent possible, the quality of available data.

How can CCOs create a sustainable process for assessing compliance risks upon changes to their business and operations?

This is very important for CCOs as well. While a compliance risk assessment is valuable on a regular basis (typically, annual or semiannual), risk profiles can change as businesses and operations change. If compliance risk is not assessed timely when there is a business change, the organization can unintentionally assume more risk than it has an appetite for.

To avoid an unintended result, it is best for compliance leaders to have "a seat at the table" when new products or services are being developed and introduced or when the organization is expanding into new geographies. This way, the compliance leader can ask questions and understand the new/emerging compliance risks in advance. The compliance leaders can assist the organization in realizing that the proposed change will breach the risk tolerance, even with mitigating controls, and also assist with the design of mitigating controls. It is important for the organization to be informed before undertaking changes to its business.

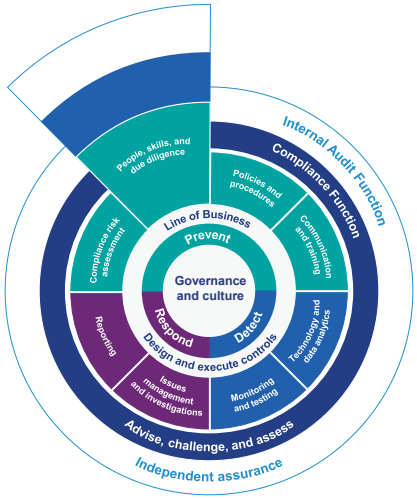
People, skills, and due diligence

Within a compliance program, proper attention must be paid to the organization's people and their skills and to instilling accountability in order for compliance objectives to be realized. In many industries, competition for compliance talent is fierce, and attrition is significant enough that it can challenge a sustainable and effective program. Given the importance of people in the control structure, it is not surprising that in KPMG's CCO Survey **55%** of CCOs identified a top compliance challenge as ensuring accountability exists and compliance responsibilities are known across their enterprise.

Instilling further accountability in employees can help to strengthen a compliance program and reinforce the culture of compliance, while at the same time mitigating risks from high turnover. Many CCOs report they address compliance infractions timely and that appropriate disciplinary actions are taken with **89%** of CCOs agreeing. However, many CCOs do not yet link adherence to compliance requirements to employee compensation or performance evaluations, which is the flip-side of what can help to further embed accountability. However, to implement this, organizations must be willing to make hard decisions, especially high-impact ones when employees that are high-revenue producers are involved in the alleged misconduct. This sends a powerful message and culturally is needed for any linkage to be effective. Perhaps for that reason, only **61%** of CCOs in KPMG's CCO Survey say that adherence to compliance policies and procedures is a factor in performance ratings and compensation decisions at their organization. Yet such a linkage can be an invaluable incentive and can go far in instilling accountability and a culture of compliance across an organization.

In addition, to mitigate risks stemming from turnover and further incorporate accountability, organizations often document the roles and assignments of their compliance personnel in the first and second lines of defense. This enables employees to better understand their roles in the compliance governance structure. Yet, KPMG's CCO Survey found that **29%** of CCOs do not have, or do not know if they have, defined and documented the compliance roles and responsibilities for employees in the first line or the second line of defense.

Ongoing skill assessments can also enable organizations to better manage compliance risks by assessing whether current employees have the requisite skills and knowledge



needed to perform their job functions and serve as strong preventive controls in preventing misconduct. This assessment exercise can also help organizations to anticipate how potential regulatory changes will impact their people, and the training and skills that they may need to provide should regulatory changes come to fruition. Here too, respondents to the Survey are struggling, with **71%** reporting that they do not have, or do not know if they have, a process for assessing compliance proficiencies and skills on an ongoing basis for their first-line and second-line staff.

Further, a more robust hiring process that includes background checks and onboarding due diligence can also help to mitigate compliance risks. These essentials appear to be widely adopted, with **82%** of organizations performing onboarding due diligence, including background checks and ongoing skills assessments, for both their employees and third-party vendors.

"Ensuring that an organization's employees and third parties understand the importance of compliance and perform their responsibilities with integrity is a critical component of an effective compliance program."

– Richard Girgenti, KPMG Principal, Advisory; Compliance Transformation Executive Sponsor

Instilling accountability: Better practices

Regulatory and evaluative frameworks suggest that organizations utilize financial and nonfinancial incentives to better hold employees accountable for compliance and support a culture of ethics and integrity. Such incentives should be:

— Tailored to the organization's business, culture, and regulatory environment

— Aimed at rewarding behaviors that support the organization's core values and expectations

— Impress on employees that compliance will have a significant impact on their careers and compensation.

One preferred way to accomplish this is to build compliance goals into performance evaluations and to evaluate employees' compliance with and adherence to those goals. Examples include:

— A percentage of a performance review rating or bonus award for a particular line of business can be tied to an employee's positive behavior aligned to corporate culture and values

— Employees can be evaluated on how well they represent their department in an ethical, informed, and courteous manner

— Employees can win a small, discretionary cash bonus or gift if their work unit achieves an agreed-upon organizational goal for a set period of time

— A corrective action process to address behaviors that do not model the entity's aspirations.

In truth, incentives and disciplinary actions will only work if they are applied consistently across the organization to all employees, regardless of the revenue they bring to the organization or their level of seniority. Thus, before embarking on this effort, senior leaders must be committed to consistent enforcement of any approach that is implemented.

CCOs agree:

Compliance infractions are addressed in a timely manner and appropriate disciplinary actions are taken — 89%

Onboarding due diligence is performed for employees and third-party vendors — 82%

However, fewer CCOs agreed that their organizations:

Factor employee compliance with policies and procedures into performance and compensation evaluations — 61%

Document compliance roles and responsibilities — 71%

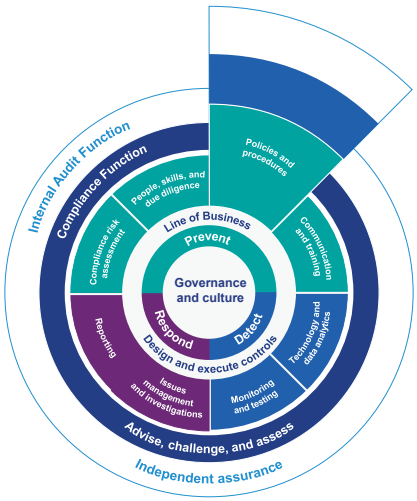
Complete regular assessments of compliance skills and proficiencies — 29%

Policies and procedures

Policies and procedures are another compliance program component that serve as a preventive control to potential misconduct. In recognition of this, KPMG has observed that many organizations have documented policies and procedures and a code of conduct. However, when organizations have documented policies and procedures that do not align fully to their implemented processes, or when the policies and procedures are not updated to reflect changes in controls, processes, or regulatory changes, this can cause confusion about how the organization intends to manage its compliance risks and the procedures to be undertaken. Compliance policies and procedures should not be "stagnant" documents—they do not reflect the state of the compliance program at one point in time. Rather they must be updated and actively maintained to support an effective program, otherwise they do little to create a consistent and sustainable approach to compliance, which is one of the primary purposes of having them.

KPMG's CCO Survey found that **84%** of CCOs have a compliance program document that provides a foundational and encompassing view of the overall program and sets forth the relevant components and applicable policies and procedures. Almost all CCOs (**94%**) report that their compliance policies and procedures are aligned with their organization's mission, vision, and values and also that compliance requirements are embedded in their policies and procedures. In addition, **95%** report they have a code of conduct that includes compliance requirements and is accessible to all employees. Importantly, **92%** of organizations also have a process in place and personnel responsible for updating their compliance policies and procedures annually or more frequently as needed.

KPMG's CCO Survey also found that many CCOs struggle with integrating regulatory change into their policies and procedures. Specifically, only **69%** of CCOs report that the compliance department has a regulatory change process in place that captures changes in applicable laws, rules, and regulations in applicable domestic and global jurisdictions. Within the consumer markets industry and healthcare/life sciences industries, organizations are even less likely to have a regulatory change process in place, with only **38%** and **54%** of respondents, respectively, indicating they have such a process.



While regulatory change is often challenging to manage, particularly for organizations operating in multiple jurisdictions, or with a diversity of product offerings and regulators, or in rapidly changing industries, it is a regulatory imperative to mitigate compliance risks. Organizations need a regulatory change management process that continually tracks potential regulations, particularly those with the highest likelihood of passage and greatest perceived impact on the organization. A robust process would also identify the business units and functional areas affected and the downstream impact on the organization's policies, procedures, processes, people, and technology that will be required to comply. While a regulatory change may appear to only impact one compliance activity, such as compliance monitoring, it is important for organizations to recognize that other compliance program areas may also require enhancement as a result—such as training, communications, or the risk assessment—and this should be incorporated into any anticipatory impact assessment and work plan.

CCOs agree:

Compliance program is documented and it provides an overview of the compliance policies and procedures

84%

Policies and procedures align with the organization's mission, vision, and values, and compliance requirements are included

94%

Code of conduct exists with compliance requirements and is accessible to all employees

95%

Process exists and staff are accountable to update compliance policies and procedures at least annually

92%

Yet, many CCOs acknowledge that they do not have or do not know if they have regulatory change process to capture changes in laws and regulations

31%

This is significantly higher in consumer markets (62%) and healthcare/life sciences (46%)

62%

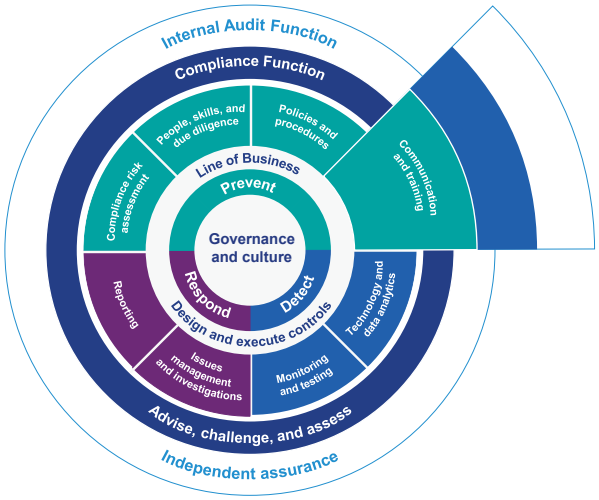
46%

Communication and training

Communication and training are core components of an effective compliance program, but how do CCOs evaluate whether their training programs are truly effective—this is a question many struggle to answer. Are longer, more content-heavy trainings more effective than shorter, more frequent and targeted trainings? Is there any correlation? How can training be used most effectively to support and enhance the compliance culture? While there surely is not one correct answer, CCOs continue to engage in efforts to refine their trainings, mature their approaches, and engage their employees amidst recognizing how adults learn and balancing training requirements against employees' other responsibilities.

KPMG's CCO Survey confirmed that most CCO respondents have a comprehensive training program in place that communicates the organization's compliance requirements and the compliance responsibilities of individual employees. Virtually all organizations (**98%**) require their employees to take compliance training on key compliance policies and procedures, and most (**94%**) provide compliance-related training to new employees appropriate to their roles and responsibilities during the onboarding process. In addition, **84%** of CCOs reported their organization has a comprehensive training program designed to provide their employees with an understanding of the current applicable key laws, rules, and regulations.

Yet one area of training that could be fruitful for CCOs to focus on further, both in design and build-out, is appropriately required training and controls of third parties. Few organizations (**43%**) reported in



KPMG's CCO Survey that they do not have, or do not know if they have, third-party vendors participate in their compliance training program or require them to complete requisite trainings. *(For further information, see Managing Third-party Risk, page 33).*

Furthermore, although **77%** of CCOs say that they have clear lines of communication within their organization so that compliance issues, lessons learned, and leading practices can be shared across the organization, **23%** do not engage in this type of open communication (or do not know if they have such an approach). Such communications can be quite valuable—reinforcing compliance perspectives and the compliance culture overall.

Communication and training (continued)

CCOs agree:

Employees are trained on policies and procedures — 98%

New employees receive training appropriate to their roles and responsibilities — 94%

The organization's training program provides employees with training on laws, rules, and regulations — 84%

However, fewer CCOs report:

Third-party vendors participate in the organization's training program or complete requisite trainings — 56%

Clear lines of communication can be enhanced to encourage lessons learned and leading practices and knowledge of issues — 77%

"I believe that trainings should be short, snackable, and shareable."

– Chris DePippo, VP, Ethics & Compliance, CSC (Computer Sciences Corporation)

Compliance training – The next generation: Better practices

Increasingly, CCOs recognize that adult cognitive learning theories support offering shorter trainings that are more memorable, engaging, and that contain real-life vignettes or stories/short videos from employees who have encountered ethical and compliance challenges. As a result, many CCOs are on a quest to innovate their compliance trainings by "freshening" their communications while still retaining the content they need to convey to employees and meet regulatory expectations. It is a balancing act. To enhance training effectiveness and limit employee fatigue, CCOs can consider:

- The results of the organization's most recent risk assessment that inform on key risks to be addressed in compliance trainings
- How to keep the content "fresh" including through storytelling, engaging with employees through a steady stream of communication "refreshers," and real examples and scenarios from the organization's workforce
- Further tailoring their compliance trainings to specific individuals based upon their job function and risk areas
- Designing or developing a training matrix that identifies, for each individual, their job function and requisite trainings
- How to train middle managers to enhance accountability and "mood at the middle" as well as to develop ethical leadership skills and knowledge of internal protocols, including for escalation of potential wrongdoing
- How to deliver compliance training content to employees who may historically only been reachable via line/in-person training using advances in technology
- Leveraging technology to monitor the results of regulatory testing to identify areas of repeat concerns and subsequently drive changes in their compliance training to match areas where regulatory knowledge appears lacking.

In addition, CCOs are:

- Utilizing technology to track training results and content distributed to employees, as well as to enable more targeted training for employees based upon their roles and responsibilities
- Considering the effectiveness of their compliance training as a mitigating control to risks in the organization's compliance risk assessment
- Incorporating weakness identified through monitoring and testing efforts into their compliance training programs to help strengthen the control environment.

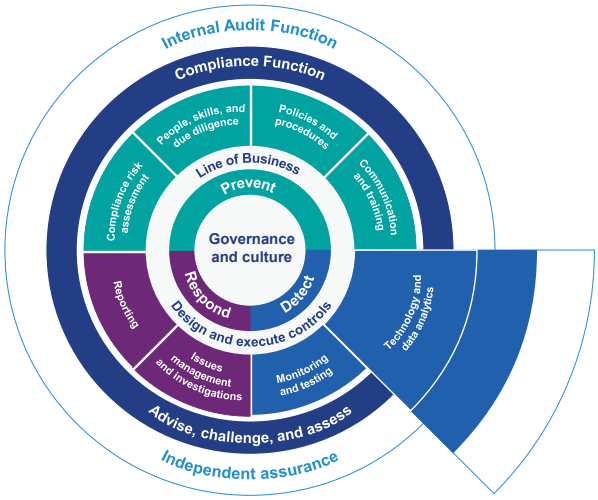
Technology and data analytics

Technology and data analytics enablement of the compliance function are necessary investments in the compliance journey that will ultimately save costs and improve performance when properly implemented as part of a corporation's strategy and operations.

Against this backdrop, it is not surprising that few CCOs report that their organization is taking full advantage of the capabilities of data analytics to support their compliance efforts. In fact, CCOs overwhelmingly report data analytics and technology as a compliance focal area. Specifically, **69%** of CCOs say their compliance program leverages technology to support its initiatives, such as compliance risk assessment, testing, monitoring, training, reporting, and documentation retention, while **31%** of organizations do not, or the CCO does not know whether their compliance program leverages technology.

Yet, significantly smaller percentages of CCOs report using the power of technology and data analytics more holistically to assess specific risks and trends or to refine their compliance activities based upon analytic results. For example, only **47%** of CCOs report using data and analytics to conduct root cause and trending analyses. Similarly, only **48%** of CCOs utilize standardized KRIs/KPIs in the development of their compliance monitoring and testing approaches and plans, and only **40%** report integrating KRIs/KPIs into their broader governance, risk, and compliance efforts at the organizational level.

Appreciating the benefits of such data analytics, many CCOs are in the process of assessing how they can further utilize their available data and derive new analytics that further their cost-effective, risk-based approach to compliance and provide more valuable compliance information to their Board. For some organizations, data remediation may be needed first in order to have available data for more valuable analytics in the future. This appears to be true for many of the respondents to KPMG's CCO Survey, as **51%** identified the need to improve data quality (for risk data aggregation and reporting) as a top compliance challenge.



For these CCOs, it is essential that needed data remediation exercises and the analytics to be developed are properly prioritized based upon the compliance strategy. All too often, CCOs get caught up in what technology and data analytics can potentially do, and fail to consider how enhancements are aligning to their overall compliance strategy, resulting in the two moving in opposite directions. Furthermore, like the compliance program overall, how an organization determines to use data analytics and technology must be right-sized for its risks, culture, and risk tolerance as well as where it is on its compliance journey.

In addition to data analytics, CCOs should also consider how their technology infrastructure supports their compliance activities and program and whether enhancements are needed. Many organizations continue to struggle with legacy technology systems or disparate systems that are the result of past mergers and acquisitions. In fact, only **40%** of CCOs report in the KPMG CCO Survey that their technology infrastructure has been analyzed to confirm that it aligns with compliance requirements and that any significant gaps have been addressed, while **39%** say their technology infrastructure is proactively adapted to align with regulatory changes and just **6%** strongly agree that this alignment occurs.

CCOs report they struggle to:

Leverage technology to support the organization's initiatives, such as compliance risk assessment, testing, monitoring, training, reporting, and documentation retention

Less than half of respondents:

Analyze whether their technology infrastructure aligns with compliance requirements and addresses any significant gaps

Use data and analytics to conduct root cause and trending analysis

Utilize standard KRIs/KPIs to develop their compliance monitoring and testing approaches

Integrate KRIs/KPIs in their broader governance, risk and compliance efforts

The volume of regulatory obligations that global organizations need to comply with continues to grow and change at a rapid pace. For more highly regulated industries, leveraging technology to manage a centralized obligations inventory is one of the ways a CCO can more efficiently and effectively monitor for changes that will impact the company's compliance obligations and related business processes and controls.

"Metrics can sometimes tell less than the full story. For instance, how do you prove things you're preventing?"

– Cynthia Patton, SVP and Chief Compliance Officer, Amgen

Regulatory change management

A systematic approach to managing compliance risks

By: Hoan Wagner, KPMG Managing Director, Advisory

Chief Compliance Officers, particularly those in global organizations, are finding it difficult to identify and manage the increasing number of laws and regulations that impact their organizations. For many CCOs, it is challenging to proactively monitor changes to the existing laws and regulations in the jurisdictions in which they currently operate, as well as to understand the laws and regulations that will result from anticipated business changes—such as expansion into new jurisdictions or new product and service offerings.

Compliance leaders recognize they need to continue to invest in their regulatory change management (RCM) programs, in order to have a sustainable approach to knowing and managing their compliance risks. For some CCOs, this means investing in and leveraging technology to automate critical areas and make data readily available throughout the organization. For others, it may mean enhancing a manual process to achieve a more consistent, repeatable, and sustainable approach to inventorying and managing regulatory changes.

The benefits of an integrated RCM process

For all organizations, a strong end-to-end RCM process allows CCOs to identify the laws and regulations that impact their organization and ultimately demonstrate that they are in compliance with the obligations of those laws and regulations. A robust RCM process also helps organizations to adapt to changes in laws or regulations and determine the impact. Minor changes might result in an update to policies and procedures, and the more significant changes may require technology enhancements or even a fundamental change in operations.

What does the RCM process include?

The RCM process should begin with the organization identifying the laws and regulations that apply to it in each jurisdiction, and should include an established process for monitoring changes. When this inventory of laws and regulations (referred to as "regulatory obligations") is undertaken centrally, the results can be accessible and shared with all divisions of the organization (as needed). A centralized process can also reduce duplication of effort and the potential for disparate outcomes by various lines of business.

As a better practice, the regulatory obligations should be drafted in collaboration with all stakeholders enterprise-wide to maintain the intent of the original laws and regulations, and written with an appropriate level of detail to enable senior leadership to understand the requirements. The dialogue with stakeholders across the organization should be ongoing so that key leaders are connected when laws or regulations change, so they can help evaluate the impact of the changes and determine the appropriate next steps.

Lessons from the financial services industry

For organizations in more regulated industries such as financial services, the RCM programs increasingly include a mapping of all laws and regulations that apply to the organization globally to its policies, procedures, and controls within any impacted lines of business. When an organization maps its regulatory obligations to its internal policies, procedures, and controls, compliance officers are better able to identify gaps in the current control environment, and they can also conduct aggregate control testing and report to the Board on their controls specific to a particular law or regulation. The accuracy of that mapping is critical to facilitate subsequent control testing, reporting, and mitigation of compliance risks. This mapping exercise can also support compliance leaders in demonstrating that they both know their obligations and have tested the controls in place to meet those obligations.

Regulatory change management (continued)

How to leverage technology to evolve the RCM process

Today, CCOs are faced with an increasingly complex regulatory landscape. In addition, many are responsible for managing manual regulatory production and compliance processes as well as increased data integrity concerns. Technology can be leveraged to help organizations to meet their regulatory requirements more efficiently and effectively. Regardless of whether an organization decides to implement an entire regulatory automation ecosystem for their end-to-end compliance needs or more targeted technology to automate specific compliance tasks, leveraging technology-based solutions helps CCOs to realize the value of compliance. Depending upon their needs, CCOs can integrate technology into their compliance programs to support a centralized oversight and governance process, automate regulatory change data feeds, and/or manage and map regulatory obligations to policies, procedures, and controls for a stronger integrated control testing framework.

Outcomes

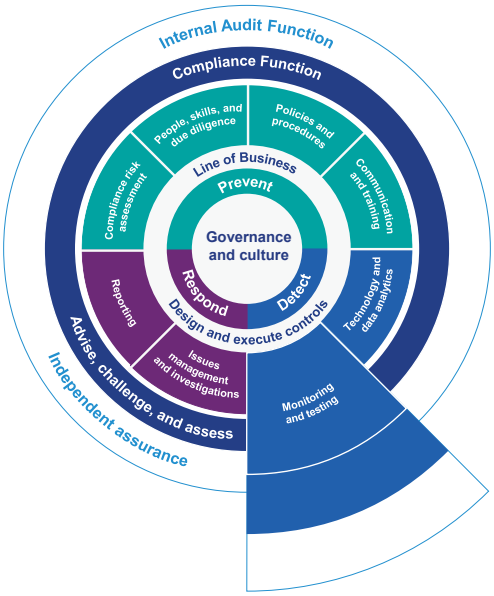
To the extent CCOs can implement a sustainable RCM process centrally, they stand to realize several benefits including a foundational (and grounded) knowledge of the laws and regulations that apply across their organization, increased efficiencies and consistency in approach, coordination with stakeholders, and potentially the ability to more proactively assess regulatory and legal changes on the horizon.

Monitoring and testing

Robust compliance monitoring and testing activities within the compliance function can be key to early identification of potential wrongdoing or risk trends, including compliance risk management control weaknesses, as well as provide evidence regarding whether the control system is operationally effective. Such testing and monitoring better positions the organization to timely detect issues and to also respond to regulatory changes that may impact the business and compliance requirements, processes, and controls. While the U.S. Sentencing Guidelines set forth suggestions for organizations to monitor and enhance their compliance programs based upon monitoring results, the suggestions do not prescribe where such responsibilities should lie or how organizations should implement such activities. As a result, outside of financial services, many organizations have targeted monitoring within their compliance functions, often for specific risks such as Foreign Corrupt Practice Act (FCPA) or third-party due diligence. Then Internal Audit completes much of the "test" work to better assess the organization's management of specific compliance risks. Many CCOs also find that monitoring and testing within their first line of defense (operations and the business units) could also be enhanced.

To this point, KPMG's CCO Survey found that many respondents could further enhance their compliance monitoring and testing programs, including for regulatory change monitoring. Of the respondents to KPMG's CCO Survey, **67%** of CCOs report having a testing program (in compliance) that performs transactional, process, and controls testing to assess adherence to compliance requirements. Further, although **75%** of CCOs agree their organization has a process in place to monitor and track regulatory changes including changes in applicable laws, rules, and regulations, only **27%** of respondents strongly agreed with this sentiment. This indicates there is room for growth in organizations' approaches to regulatory change monitoring.

Outside these areas, CCOs tended to report that they have open lines of communication with senior management, their Board, and management regarding their



monitoring efforts. Specifically, **74%** of organizations say they communicate compliance testing results to senior management and a Board committee. Such reporting provides essential information for the Board and senior management. In this way, organizations assist leadership in their oversight responsibilities and management of risk.

Furthermore, **84%** of KPMG CCO Survey respondents say they use compliance monitoring results to develop action plans, and they monitor progress and completion of committed actions. Such an approach furthers the organization's ability to identify necessary enhancements to specific controls or processes in order to further mitigate identified risks. Some organizations have implemented Enterprise Risk Management (ERM)-type dashboards to report and track their risks and specific compliance monitoring and testing results, including the level of the risk, senior-level ownership of the risk, the status of monitoring and testing results, and action items. *(For further information, see Reporting, page 30).*

Monitoring and testing (continued)

CCOs agree:

Report compliance monitoring results to senior management and a Board committee — 74%

Use compliance monitoring results to develop action plans, and track progress and completion of committed action — 84%

CCOs report they do not, or do not know if they perform transactional, process, and control testing in their compliance functions — 33%

Only 27% of CCOs strongly agree that they monitor and track regulatory change. — 27%

"Establishing a centralized compliance testing team can help an organization to enhance its governance and oversight of compliance, including through better aggregation of test results and, consequently, more comprehensive data analytics."

– *Todd Semanco, KPMG Partner, Advisory*

Enhancing your compliance effectiveness and agility through monitoring and testing activities: Better practices

Action steps that compliance leaders can consider in order to improve their compliance monitoring and testing effectiveness include the following:

Consider your compliance risk assessment

Provides compliance leaders with a basis for defining their compliance risk universe in a consistent manner and can assist compliance leaders in identifying priority risks, including emerging risks, for inclusion in the testing plan. Compliance leaders can also use the compliance risk assessment to more finely and strategically target specific areas of risk including business units, operations, or products that pose higher risk, for more frequent and intensive testing.

Delineate roles and responsibilities

Delineation of monitoring and testing roles and responsibilities across all three lines allows stakeholders to see the whole picture of how they execute testing and monitoring activities across the organization, helping to identify efficiencies, reduce duplications, and more effectively identify higher-risk control gaps or problems more timely. Implementing monitoring and testing activities within the first line also helps to instill greater accountability.

Compliance functions are increasingly reliant upon technology

From the way organizations monitor and manage global changes, to regulatory obligations and how testing is performed, analyzed and reported, all components of managing the function are under review. The demands, from internal and external stakeholders alike, to demonstrate adequate coverage and provide precise impact and root cause analysis are very high. To meet these demands, leaders are increasingly turning to technology to collect, consolidate, and map key data elements together—for example, obligations, policies, risks, controls, process detail—at a granular level. This capability supports not only dynamic regulatory change management activities, but also the oversight of business process and technology changes. Further, by consolidating and integrating monitoring and testing scripts within this technology, forming rules engines, outcomes, and impacts may be more immediately assessed and remediated while data is accumulated to support predictive analytics.

In addition, some recent trends in the scope of compliance testing and monitoring programs include:

- Third-party relationships
- Compliance policies and procedures to assess alignment to the organization's implemented processes
- Consumer/customer complaints that could reflect trends indicative of harms or misconduct
- Emerging compliance risks
- Root cause analysis and impact assessments of monitoring and testing results
- The integration of digital labor and establishment of enterprise-wide automation infrastructure.

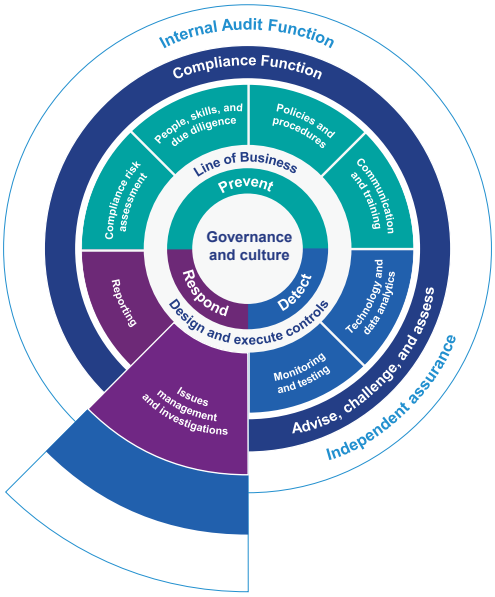
Issues management and investigations

Even the most well-designed compliance program can encounter wrongdoing or compliance risks that require it to have an effective mechanism for responding. This includes protocols and mechanisms for investigating escalated activity and more broadly for all issues management (e.g., regulatory inquiries, subpoenas, or a crisis).

Many organizations recognize that investigation results of substantiated misconduct can be used to look for patterns and identify root causes, which can help the organization take appropriate corrective actions. The results can also be used as an indicator of whether issues are systemic or instead cluster in certain organizational levels or departments. KPMG's CCO Survey found that most organizations employ investigation results and metrics in this way including to identify and prioritize enhancements to the program. For example, **77%** of CCOs say their organization uses investigation results and metrics to inform and prioritize enhancements to the compliance program. In addition, **65%** of organizations have a process in place to assess the impacts of issues, identify root causes, assess any cross-organizational impacts, and create enterprise-wide solutions.

Furthermore, since investigation results often can provide important insights indicating whether the compliance program is effective, key statistics and trends should be reported to the Board to assist in their oversight responsibilities. KPMG's CCO Survey found that most CCOs do so, with **76%** of organizations indicating that they report to the Board at least annually on investigation metrics, including quantitative data and root cause analysis.

KPMG CCO Survey respondents differ with regard to how they structure their investigations and issues management approaches and whether they team and involve other functions in their efforts. Most organizations



report that their issues management and investigations are centralized, although a significant minority still follow a decentralized approach. Specifically, **71%** of CCOs report that they have a centralized issues management process and structured coordination with other groups such as ERM, Internal Audit, general counsel, HR, and corporate security, while **71%** also say they have a centralized investigative unit with structured coordination with other groups. Regardless of the approach an organization selects—centralized, decentralized, or a hybrid approach—it is important that information flows upward and risk trends can be aggregated and understood. The structure chosen should also be appropriate and risk-sized for the organization, including based upon its business, operations, and geographic presence.

CCOs agree:

Investigation results and metrics inform program enhancements — 77%

Annual reporting of investigation metrics to the Board occurs, addressing root cause analysis and quantitative data — 76%

Processes are in place to assess the impact of issues, root causes, and cross-organizational impacts and to create enterprise-wide solutions — 65%

They have centralized issues management and investigative processes, and have implemented and structured coordination with other groups such as ERM, Internal Audit, general counsel, HR, and corporate security — 71%

Enhancing investigation effectiveness: Better practices

Below are areas and better practices for an organization seeking to enhance their investigation effectiveness.

Best practices

Strong investigation culture – Compliance leaders view confidentiality as a crucial aspect of a successful investigation culture. Handling investigations in a respectful way is also growing in importance as CCOs recognize the need to maintain an effective and positive environment while uncovering the facts.

Protocols – Given the recent YATES Memo,[8] some CCOs are also taking the opportunity to review their protocols and their escalation matrices to assess if any enhancements or changes should be undertaken. Protocols, including investigative methodologies, that contain direction and guidance are essential foundational elements for internal investigations and help to create a consistent and sustainable approach.

Trainings – Leading practices in training programs for investigators include utilizing investigative fact patterns that are carefully scripted—and role playing to practice interviewing techniques as well as to address common errors commonly observed based upon quality assurance reviews and/or audit feedback. Further, trainings should include updates to investigation protocols, structure, or communications approach, in order to encourage prompt application and integration.

Technology – Fundamental to an investigations program is an organization's ability to *know* the fraud and misconduct allegations and to hone in on KRIs. To yield valuable intelligence on the state of investigations, escalated issues, and risk factors, organizations should have a dashboard feeding in from all relevant systems. Yet, only 3% of organizations report they use proactive antifraud data analytics in detection of the fraudsters surveyed.[9] Data analytics is a key antifraud technology utilized to sift through millions of transactions looking for suspicious items.

Root cause analysis – Root cause analysis, or post-investigation analysis, assists organizations in identifying qualitative measurements and create a feedback loop on what is learned during investigations. Root cause analysis may include a review of increases in certain types of HR-related cases or cases in specific jurisdictions, or repeat inquiries about the same employee. This analysis helps the organization to understand what could be driving certain behaviors, enable implementation of appropriate corrective actions to address the root cause(s), enhance stakeholders' understanding of the trends identified, and improve organizational performance.

8 Source: Department of Justice Memorandum, Sally Quillian Yates, Individual Accountability for Corporate Wrongdoing, http://www.justice.gov/dag/file/769036/download

9 Source: KPMG Survey, Global Profiles of the Fraudster, May 2016, found that 44% of fraudsters were detected as a result of a tip, complaint, or formal whistle-blowing hotline; a further 22% were detected as a result of a management review. This further evidences the need for confidentiality and a strong investigative culture.

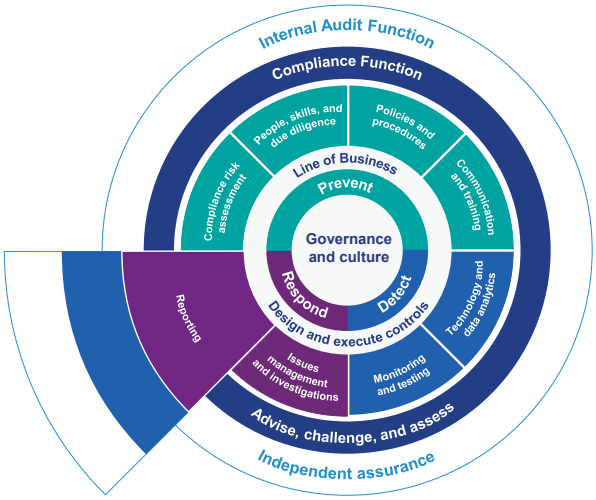
Reporting

Organizations must have effective reporting mechanisms in order for the governing authority in the organization, such as the Board, to be knowledgeable about the compliance program in place and exercise reasonable oversight of the program, as well as to manage compliance issues that could require external reporting. Individual(s) with operational responsibility shall report periodically to the governing authority, or an appropriate subgroup, and high-level personnel on the effectiveness of the compliance and ethics program.

To this end, CCOs report to the Board, or subcommittee of the Board, on their key compliance risks, and the controls they have in place to manage these risks, including monitoring/testing of the controls across the three lines of defense. In addition, many CCOs report to their Board on internal (and possibly external) compliance trends, which are supported by investigation metrics, training metrics, and disciplinary statistics as well as on external changes in the regulatory environment.

Most CCOs report in the KPMG CCO Survey that their organization has compliance reporting that addresses these issues. Specifically, **84%** of organizations report to their Boards on the enterprise-wide state of compliance including culture, conduct, governance, and key issues. In addition, **83%** of CCOs believe compliance reporting supports the organization's risk appetite framework and strategic efforts to meet heightened expectations for risk management.

Although most organizations have reporting processes in place, only **47%** of CCOs indicated that they have an integrated reporting system across their organizations (e.g., business units, operations, IT, issues management, and complaints), which includes compliance monitoring. When an organization's technology infrastructure is vast and decentralized, CCOs can be challenged to obtain data, as well as consistent data, to evaluate risk exposure. This then limits the CCO's and other senior leaders' vision



of the organization's compliance risks on an enterprise-wide basis. Often times, organizations try to mitigate this through manual efforts and aggregation, and some are utilizing governance, risk, and compliance (GRC) technology, although it is not a perfect fit. Consequently, CCOs chatter about the need for a common reporting dashboard utilized across an enterprise, with data feeds in from disparate sources, to enable an aggregate view of compliance risks that can also be shared with their Board and other senior leaders.

KPMG is currently assisting clients with leveraging technology to build an inventory of U.S. and regional regulatory requirements impacting their global products, services, and legal entities. This technology will allow organizations to obtain updated laws and regulations from agreed-upon sources and provide information at a frequency defined by KPMG and the client. As organizations further integrate and automate their processes, these types of technologies will allow compliance stakeholders to have real-time management of their regulatory obligations as they further evolve and mature.

CCOs agree:

They report to their Boards on the enterprise-wide state of compliance including culture, conduct, governance, and key issues

Compliance reporting supports the organization's risk appetite framework and strategic efforts to meet heightened expectations for risk management

Yet, only 47% of CCOs say their enterprise-wide reporting system is integrated across the organization (e.g., business units, operations, IT, issues management, and complaints) and includes compliance monitoring

"Reporting can feel like putting a puzzle together, and CCOs should be mindful that those contributing to the puzzle may not know how the pieces all fit together. Sharing the 'cover of the jigsaw puzzle box' can help them see how they fit into the overall picture. Just the same, report recipients may not fully understand the big picture until all of the reporting pieces are finally assembled in one place."

– Ben Bard, VP & CCO, Archer Daniels Midland

Implementing a reporting dashboard

By: Tom DiLeonardo, KPMG CCO

As KPMG's chief compliance officer, it is among my responsibilities to provide the firm's leadership committees with useful information on our ethics and compliance efforts, including various trends emanating from our internal investigations. However, given the voluminous amount of data maintained in the firm's investigations database, analyses and assemblage of such information has presented challenges over the years. Initially, the information contained in the database was tediously analyzed and assembled by hand. Over time, we automated the process, and we now use a customized "dashboard" software program that accesses the database information, automatically performs data and trend analyses, and assembles the information directly into a management reporting deck. This automation has improved our efficiency.

Automating reporting dashboards and KRIs/ KPIs: Better practices

In an environment of rigorous regulatory enforcement measures, compliance program effectiveness is a priority focus area for management, Boards, and audit committees. A reporting dashboard can provide valuable insights regarding the state of a compliance program operations and overall effectiveness enterprise-wide. It should also be comprehensive, including more than just monitoring and testing results or the status of only high-risk areas of concern. For example, it should include compliance activities such as:

- **Investigations** – Analytics relating to open and closed cases reported through ethics and compliance hotlines and other channels
- **Training and certifications** – Analytics focused on employee training compliance and required certification renewals
- **Due diligence** – Analytics focused on key personnel and vendor decisions
- **Retaliation monitoring** – Analytics focused on monitoring the career paths of personnel who have been participants in a prior or current investigation
- **Monitoring and testing** – Results including open items that are being tracked to completion, repeat issues, and identification of ownership for each item and due dates
- **Performance management** – Statistics linked to compensation and rewards based upon employee compliance.

In addition, applying enhanced, forward-looking metrics and conducting a quantitative analysis can better showcase a comprehensive view into the enterprise-wide state of compliance.

Data integrity and governance play a fundamental role in reporting as these directly correlate to the organization's ability to consistently report with a high degree of accuracy.

The challenge of managing third-party risk

Organizations today face rising global regulatory expectation and scrutiny of their third-party relationships, which is impelling many to enhance their third-party risk management controls, monitoring approaches, and resources. As a result, organizations tend to conduct a more in-depth and risk-based examination of counterparties when they begin relationships, monitor relationships on an ongoing basis, and provide for offboarding counterparties based upon their monitoring and assessments of risks. As CCOs recognize, failure to adequately assess their agents, business partners, and clients and how they operate, can expose CCOs not only to operational risk, but also to costly government investigations and reputational damage, which is often hard to measure, as well as monetary penalties and potential criminal liability. Yet, as KPMG research has found, it is challenging to oversee and control third parties, which may be one reason that third parties are involved in more than 75 percent of corruption cases.[10]

However, a significant portion of CCOs participating in KPMG's CCO Survey report that they have not implemented leading practices to manage their third-party compliance risk. Specifically, while **82%** of organizations conduct onboarding due diligence for employees and third parties, including background checks, only **51%** of CCOs report that they have a process to confirm that third parties adhere to compliance due diligence processes and all but a few (**13%**) identified they have room for growth here. Further, only **56%** of organizations report that they require their third parties to participate in compliance training when engaged and on an annual basis thereafter, if appropriate. Furthermore, only **31%** have an enterprise-wide tool that they employ to manage their third-party risks, and which is capable of providing KRIs/KPIs, and tracking issues. Given the need for organizations to implement a consistent and sustainable risk-based approach to managing their third-party risks, having an adequate technology infrastructure to support their efforts is essential. Some benefits to implementing a technology infrastructure to support third-party risk management (and preferably at a centralized corporate level) can include automated controls, risk rating functionality, audit trails, repository of third-party documentation, testing results, and better overall support of the lines of business through a more efficient onboarding and monitoring process (and potentially better contracting terms).

For some organizations, the technology infrastructure currently utilized to manage third-party risks is decentralized while for others it is centralized. Often times, this correlates to the third-party risk management governance structure in place. Irrespective of the approach taken, an organization's program for managing its third-party risks must be right-sized in order to be effective and sustainable. In addition, to be truly valuable to the organization, the more agile the approach is, the better, as third-party risks can evolve and change.

10 Source: OECD Foreign Bribery Report: An Analysis of the Crime of Bribery of Foreign Public Officials, OECD Publishing, 2014.

CCOs agree:

They conduct onboarding due diligence for employees and third parties, including background checks

82%

Yet only:

— 51% have a process to confirm that third parties adhere to compliance due diligence processes

51%

— 56% require their third parties to participate in compliance training when engaged and on annual basis thereafter

56%

— 31% have an enterprise-wide tool that they employ to manage their third-party risks, and which is capable of providing KRIs/KPIs, and tracking issues

31%

Managing third-party risks: Better practices

By: Graham Murphy, KPMG Principal, Advisory

Recently, we have seen considerable regulatory activity and guidance put forward by regulators. New anti-bribery and corruption laws have been implemented in many jurisdictions, including in 2015 in Brazil, 2013 in Canada and Russia, and the U.K. Bribery Act of 2010. In late 2012, the U.S. Securities and Exchange Commission (SEC) and Department of Justice (DOJ) issued a resource guide for the U.S. Foreign Corrupt Practices Act (FCPA), which included guidance to help organizations with how they manage third parties.

In this regulatory climate, a strong program for managing third parties needs to include elements of prevention, detection, and response. Since an organization cannot prevent every situation from arising, it needs to establish protocols to detect when a potential violation has occurred and to respond appropriately to that situation. From a prevention standpoint, the objective is to understand the nature of the government touchpoints that exist across its various markets and to reduce incidents by negotiating clear contracts with appropriate anti-bribery and corruption language, undertaking third-party education and training, and, of course, performing appropriate third-party due diligence. In terms of detection, hotlines or other reporting channels are a starting point, but more organizations are now going in-country to perform site visits and reviews. These efforts are aimed at understanding whether their programs on paper are, in fact, functioning properly.

The challenge for many organizations today is that they may have thousands or tens of thousands of third parties and they must determine how to assess which third parties present the greatest risk and what level of effort, including due diligence, should be applied. The real risk lies in the people operating third-party companies—people pay bribes, not companies—so often, the due diligence an organization conducts needs to also examine the individuals behind the entities, including officers, directors, and perhaps shareholders.

Today, technology solutions are available to help companies organize their third-party compliance program and create a sustainable and consistent approach to performing due diligence and enhance third-party risk management effectiveness and efficiency. The technology solutions are often a part of a broader governance, risk, and compliance, or GRC, suite of solutions. The technology solution needs to be customizable to the company's policies, procedures, and processes and should be flexible to support the organization's unique requirements relating to risk rating and escalation protocols.

Regulatory expectations for how organizations manage their third-party risks are rising and to be equipped, CCOs must proactively assess how their current program measures up, and what, if any, better practices they can consider implementing as they mature their programs and continue in their compliance journeys.

"For some companies, brand is everything, and a third-party issue can drive away customers, make investors nervous, cause a decline in stock value, and damage the company's ability to attract top talent."

– Graham Murphy, KPMG Principal, Advisory

In summary

Although the regulatory landscape, particularly in the United States, continues to evolve, the fundamentals of what regulators expect from a compliance program remain—an effective and sustainable program for preventing, detecting, and responding to potential misconduct. Therefore, in the midst of this uncertainty, CCOs can remain focused on how to further improve their compliance program in order to **comply** with existing regulations and expectations. Using their internal enterprise-wide compliance risk assessment, CCOs can identify potential control gaps, control weaknesses, and risk trends for prioritized enhancement.

To remain competitive, CCOs may also identify and prioritize enhancements in their compliance activities that will enable them to become more efficient and agile, which typically occurs from further **integration** and **automation** of the compliance program across the organization.

In addition, CCOs can benefit from having a five- and ten-year plan that projects what their future compliance program will need to look like, based upon existing regulatory and enforcement action trends, and continue to invest in foundational elements for this future program.

Appendix

Profile of respondents

The organizations participating in KPMG's CCO Survey operate in the following industries: consumer markets (13%); energy and natural resources (14%); financial services (34%); healthcare and life sciences (21%); industrial manufacturing (8%); and technology, media and telecommunications (10%).

Respondents also described their compliance departments/functions as having a range of sizes including less than 25 professionals (40%), 25 to 74 professionals (23%), 75 to 250 professionals (21%), and more than 250 professionals (16%).

Furthermore, 48% of organizations report that the head count of the compliance department increased over the past year, while 19% report it decreased, and 32% say there was no change. Roughly 60% of CCOs report that the compliance function budget at their organizations increased in 2014 (60%) and 2015 (57%), and 48% report an increase in 2016. In contrast, only about one-third of CCOs expect continued increases in budgets going forward.

Acknowledgments

Compliance Transformation Team

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

Julie Gerlach
Managing Director, Advisory Compliance Transformation Solution National Co-leader
T: 404-222-3389
E: jgerlach@kpmg.com

Richard Girgenti
Principal, Advisory
Compliance Transformation Solution Executive Sponsor
Americas Forensic Leader
T: 212-872-6953
E: rgirgenti@kpmg.com

Kari Greathouse
Technology, Media and Telecommunications Lead
T: 314-244-4096
E: cgreathouse@kpmg.com

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

Amanda Rigby
Industrial Manufacturing Lead
T: 312-665-1953
E: amandarigby@kpmg.com

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

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

Jennifer Shimek
Healthcare and Life Sciences Lead
T: 973-912-6167
E: jshimek@kpmg.com

Tim Hedley
Consumer Markets Lead
T: 203-406-8420
E: thedley@kpmg.com

Authored by Nicole Stryker, with editorial review by Karen Staines and additional contributions from the following:

Swati Austin
Deborah Bailey
Melissa Blutstein
Rob Bryant
Elizabeth Byrum
Regina Cavaliere
Ori Ben-Chorin
Tatum Crotinger
Rob Haney
Graham Murphy
Jaime Pego
Rob Ranley
Todd Semanco
Hoan Wagner
Michael Wegh

kpmg.com/socialmedia

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