Deloitte.

An Insurer's Guide to the DOJ's Guidance for Effective Compliance Programs

Key features of the updated guidance – and steps for insurance companies to consider for their Compliance Programs

In the summer of 2020, the US Department of Justice (DOJ) issued its updated Evaluation of Corporate Compliance Programs (CCP). Supplemented by the Federal Sentencing Guidelines, the updated guidance reflects the increasing sophistication expected by regulators to demonstrate that the CCP in both design and in practice works effectively.

The updated guidance outlines the heightened regulatory expectations around important CCP elements: program structure, autonomy, and resources; risk assessments; testing and monitoring; internal investigations; training; confidential reporting; M&A; and third-party programs. Compliance and risk professionals should not only be aware of these updates, but should also evaluate what, if any, steps their companies should take in response, now and over time, as there is an expectation of continuous program evaluation and refinement. This point of view highlights some expectations in several of these elements and provides considerations for how insurers may address them.

In general, the DOJ's expectations continue their trend toward driving greater program sophistication and demonstrating effectiveness. Further, it implies that companies may need to make on-going enhancements and investments in their compliance programs. Enhancements and investments will need to be thoughtfully prioritized and incorporated into the existing compliance program, in a risk-based, cost-effective manner while avoiding unnecessary procedural complexity, reducing silos and redundancies, and aligning resources and activities to areas of greatest importance.

Although this may appear self-evident, there is frequently a mismatch between how resources are aligned to the company's risks.

Guiding Principles: Culture, Design, Implementation, and Effectiveness

In the updated CCP, the DOJ emphasizes the need for compliance programs to be "well-constructed, effectively implemented, appropriately resourced, and consistently enforced." Further, the DOJ wants to see that the compliance programs were effective "at the time of the misconduct and at the time of the resolution." At a practical level, these expectations impact a number of activities, discussed below.

Creating a Culture of Compliance and Ethical Behavior

The underpinnings are a deeply rooted culture of compliance and ethics throughout the organization. In the guidance, the DOJ will examine not only the Senior Management commitment, but also examine how Middle Management reinforces it in the day-to-day practices. Because of this, setting and reinforcing the correct tone from the top of the organization is critical for the success of a program. The messaging can take many forms, but company leaders and managers should continually remind its employees through townhalls, newsletters, emails, and postings around the office of each employee's responsibilities as it relates to compliance. Accountability is driven through all levels and all functions. Confining the messaging and responsibility within the boundaries of the compliance department is not enough.

Steps to Consider: Being intentional in your compliance messaging is essential to setting a compliance-focused culture. On-going oral and written communications from the company's leaders and managers are important and effective. Many insurers are increasingly promoting compliance and ethics through their company websites, highlighting compliance events, reminders, and upcoming training to engage the broader employee base and create more compliance and ethics-motivated mindset. An effective but underused technique is conducting an annual Compliance survey of all employees to assess the effectiveness of compliance-related activity in the organization. Annual surveys provide valuable insights on how messaging is working as well as other indicators of potential issues or misconduct.

Strong emphasis on structure, autonomy and resources

The CCP emphasizes that a compliance program's structure, autonomy, resources, and the foundational question of whether the company is applying the compliance program "in good faith." This question is also geared to determine whether "the program is adequately resourced and empowered to function effectively."

In addition, the CCP states that the DOJ will seek to understand "why the company has chosen to set up the compliance program the way that it has," "the reasons for the structural choices the company has made," and "how the company's compliance program has evolved over time." The organization model for the compliance function is frequently one of the biggest challenges for insurers and directly impacts operational effectiveness and efficiency.

Companies will need to look to share resources as much as possible in order to meet budgetary restraints. With that in mind, Compliance officers will then need to take a critical look at their own people to ensure their team meets the challenges of their current risk framework with the appropriate knowledge and expertise.

Steps to consider: Companies should strongly consider documenting the evolution of their respective compliance programs. This includes all changes made and the reasons for the changes. Even with a formal system to document the program evolution, it can be challenging to effectively demonstrate —often years later and with leadership and model changes—the good faith efforts undertaken by the compliance team to improve the program.

Additionally, companies should assess if all of the activities that compliance is responsible for are appropriately assigned, or if those activities would be better suited for first-line supervisors. Increasingly, more operational activities are being assumed by first line business functions, such as licensing, registrations and appointments, rate and form filings, and complaint handling. Compliance continues to provide regulatory guidance, conduct monitoring and risk-based testing.

Formalizing the three lines of defense control model for effective application of the Compliance Program

In answering the question posed by the DOJ to understand the rationale for a company's compliance program structure, it is appropriate to consider the definition of responsibilities among the first line (business owners), second line (compliance and risk) and third line (internal audit). It is not uncommon that the lines and responsibilities between first line supervisor and compliance or risk are blurred in insurers.

Steps to Consider: Companies should strongly define the supervisory responsibilities and procedures it expects from the first line. By providing first line supervisors with the authority to pragmatically solve challenges and with the supervisory responsibilities for the day-to-day operational performance, Compliance can be better positioned to provide independent monitoring, testing, and constructive challenge to gauge that controls and reporting are effective.

Meaningful risk assessments

The DOJ has established that risk assessments are the foundational element of the compliance program, although in practice this element often lacks the expected degree of rigor. The assessment itself is often a process that is inconsistently applied, without the desired engagement of business and other key stakeholders. Additionally, it is common in the insurance industry to not conduct risk assessments on a regular basis or to fully consider root-cause drivers. The guidance considers whether "the company had identified, assessed, and defined its risk profile, and the degree to which the program devotes appropriate security and resources to the spectrum of risks." Additionally, the DOJ stated that it will now assess whether the organization's periodic risk assessment is "limited to a 'snapshot' in time or based upon continuous access to operational data and information across functions."

The DOJ also indicates the importance of having a process to track and incorporate lessons learned into the risk assessment. This shows that risk assessment is a closed-loop process, linking results from monitoring, testing, and investigations as well as root cause analysis to the risk assessment.

Steps to consider: Companies should consider how changes in their business impact their risk assessment by incorporating lessons learned from investigations, whistleblower reports, M&A activity, and other internal and external events. Companies may track key compliance risk metrics from various data sources between periodic risk assessments to identify trends and patterns of risk. For example, with an increased focus on protecting consumer data, information technology risk should be consistently tracked for breaches, phishing attempts, and other exposure to unwanted activity with real-time notifications to relevant internal stakeholders to address and remediate any potential area of concern. Similarly, compliance surveys are an effective leading indicator to highlight parts of the company where there may be gaps in desired leadership behaviors.

While there is no one correct approach to a risk assessment, Insurers should expect compliance to drive a risk assessment, no less than annually, which includes interactions with business partners and key control functions such as Risk and Internal Audit. It is designed to use a risk-based approach that evaluates the controls in place across the company. The determined risk universe should be regularly reviewed and updated as prosecutors will consider whether the company has analyzed and addressed the varying risks presented by—among other factors—the location of its operations, insurance industry issues, the regulatory landscape and applicable set of laws and regulations, clients and business partners, transactions with foreign government entities, payments to foreign officials, use of third parties, gifts, travel, and entertainment expenses, and charitable and political donations.

Periodic Testing and Review – Use of Data in Assessing Effectiveness

For an organization to be able to demonstrate effectiveness, it "should take the time to review and test its controls." The DOJ guidance is more detailed here and emphasizes access to and use of data for monitoring, testing, and assessing effectiveness. For example, the CCP now asks, for the first time, whether "compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions?" It also now asks whether "any impediments exist that limit access to relevant sources of data and, if so, what is the company doing to address the impediments?"

Yet the DOJ is concerned not only with access to data, but also with how data is used in compliance activities such as assessing the effectiveness of training, whistleblower hotlines, investigations and disciplinary actions, third- party lifecycle monitoring, and post-M&A internal audits – among others.

Another change to the CCP describes a new expectation that companies cast a wider net when using lessons learned to enhance their risk management frameworks. Specifically, the DOJ added language to emphasize reviewing and adapting compliance programs based on lessons learned not only within the organization but also those of other companies "facing similar risks."

As companies consider the impact of the guidance, it is likely to accelerate the industry transformation on developing increased data analytics and resources with industry, regulatory, and data skills.

Steps to consider: Companies should take a fresh look at their monitoring and testing procedures to determine how they align with their risk assessments, to ascertain not only whether they are well-designed and "applied earnestly and in good faith," but also whether the compliance program is, in actual practice, effective. This may include considering ways of incorporating lessons learned from entities facing similar risks, such as industry peers and through the insurance industry forums, as well as from internal audit and risk management within their own organization.

Regarding structural impediments to the access and use of data for monitoring, testing and compliance risk measurement, companies that divide these responsibilities among various functions and units should take steps to break down the silos among those groups, particularly those that could limit effective data access and its use for robust data analytics and the application of such information to identify risks and program improvements.

Post-remediation root-cause analysis for further enhancements

Infractions do and will continue to occur in companies, even in the best compliance programs. It is the role of compliance to prepare companies to be thoughtful and proactive to determine where such issues may arise and to respond to remediation efforts swiftly, appropriately, and ensure that same issue does not occur again.

The evolution over time and showing lessons learned are important to the DOJ. The CCP asks prosecutors to assess why and how an institution has evolved its compliance program over time and, as part of this evolution, how it has leveraged "lessons learned" in enhancing the risk management framework. A hallmark of a compliance program that is working effectively in practice is the extent to which a company is able to conduct a thoughtful root cause analysis of misconduct followed by timely and appropriate remediation.

Prosecutors evaluating the effectiveness of a compliance program are instructed to reflect back on "the extent and pervasiveness of the criminal misconduct; the number and level of the corporate employees involved; the seriousness, duration, and frequency of the misconduct; and any remedial actions taken by the company, including, for example, disciplinary action against past violators or remedial changes to policies, procedures, systems and training."

Prosecutors will assess whether the company has clear disciplinary procedures in place, enforces them consistently across the organization, and ensures that the procedures are commensurate with the violations.

By identifying root causes and addressing foundational issues within the compliance framework, the compliance team can demonstrate a tangible response and appropriate remedial response. The Federal Sentencing Guidelines advise that consideration be given to "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision" and the corporation's remedial efforts "to implement an adequate and effective corporate compliance program or to improve an existing one."[1]. This would include considerations for what the company had in place at the time of the misconduct for the purposes of calculating the appropriate organizational penalty.

Additionally, the DOJ guidance elaborates that prosecutors when performing an assessment will assess, "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as the time of a charging decision" and the corporation's remedial efforts "to implement an adequate and effective compliance program or to improve an existing one."

Steps to consider: Continuous improvement should consistently be in the forefront of an insurer's compliance strategy. Prosecutors will consider whether the company has engaged in meaningful efforts to reviews its compliance program and to determine that it is relevant and effective. This includes program revisions in light of lessons learned and to drive sustained

[1] United States Federal Sentencing Guidelines 9-28.300

improvement. Root cause analysis provides an organization the opportunity to fully examine a violation and address the underlying issues in the program itself; learning from incidents and trends and patterns are crucial in the ongoing refinement of any compliance program.

Increasing Importance of Internal Investigations

New language by the DOJ in the CCP emphasizes the importance they place on a company's response to potential misconduct:

"The truest measure of an effective compliance program is how it responds to misconduct. Accordingly, for a compliance program to be truly effective, it should have a well-functioning and appropriately funded mechanism for the timely and thorough investigations of any allegations or suspicions of misconduct by the company, its employees, or agents. An effective investigations structure will also have an established means of documenting the company's response, including any disciplinary or remediation measures taken."[2]

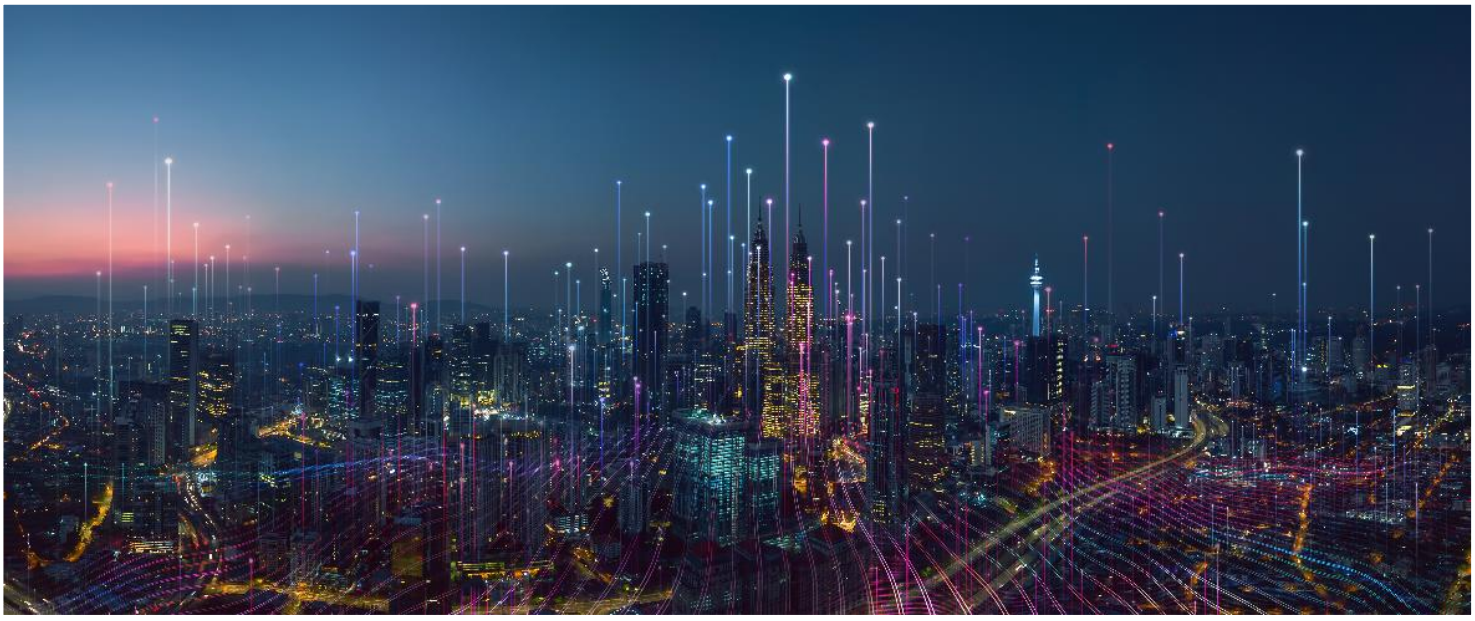
Further emphasizing the importance of consistent discipline after investigations, the guidance notes that the DOJ expects "the compliance function [to] monitor… investigations and resulting discipline to ensure consistency." Prior changes to the CCP also emphasize the importance of considering appropriate discipline for supervisors – not only those identified "as responsible for the misconduct, either through direct participation or failure in oversight," but also for having "supervisory authority over the area in which the criminal conduct occurred."

Steps to consider: The guidance emphasizes the importance of well-scoped investigations, root cause analysis, and appropriate remediation in light of lessons learns including disciplinary actions. Therefore, companies should review how investigations are handled from initiation through completion, as well as any resulting improvements from such assessments. Insurance companies that reinforce positive employee behavior can help drive a stronger culture of ethics and compliance as outlined in the Federal Sentencing Guidelines.

M&A Due Diligence

The DOJ suggests that compliance programs should continue to apply a risk-based approach when it comes to its due diligence procedures. For various M&A transactions, a well-designed compliance program for an insurance company should include comprehensive due diligence of any acquisition targets, as well as a process for timely and orderly integration of the acquired entity into existing compliance program structures and internal controls. Pre-M&A due diligence, where possible, can enable the buyer to evaluate more accurately each target's value and negotiate for the costs of any corruption or misconduct to be borne by the target.

Steps to consider: As part of a formal M&A playbook, insurers should consider assessing the compliance needs and capabilities of any acquisition target as a part of a pre-M&A due diligence process. Providing the compliance team an opportunity to understand post-merger regulatory expectations and synergies within the current program framework can drive a smoother transition and ideally open the door for sooner realization of post-merger benefits (e.g., minimizing redundancies, optimizing costs, and managing new risks).



[2] "Evaluation of Corporate Compliance Programs" (2020)

Confidential reporting

Consistent with a key theme of the updated guidance documents, the DOJ's CCP provides additional context as to what constitutes effective confidential reporting mechanisms such as whistleblower hotlines. The DOJ will ask whether companies "periodically test the effectiveness of the hotline, for example by tracking a report from start to finish." The DOJ also views effective hotlines as ones where "employees are aware of the hotline and feel comfortable using it" and wants to see companies taking measures to test this.

In one final change, the DOJ calls for publicizing the reporting mechanism, not just to company employees but to "other third parties."

Steps to consider: Companies should consider conducting periodic testing of whistleblower mechanisms, such as hotlines, as part of the overall risk-based testing of compliance programs. Today, many companies have some level of testing with a specific focus on entity-level controls (ELCs). The updated guidance further emphasizes the need for an effective hotline mechanism and program. Further, in an effort to ascertain employees' and other potential users' views of those mechanisms, it may be useful to use anonymous surveys to assess employee awareness, comfort, and concerns about use of the hotline, their trust in the investigation process, and any potential retaliation. It might also be useful to assess whether calls are coming in, proportionately, from all areas of the business and countries of operations.

Effectiveness is the goal

In light of the DOJ's CCP, it may be more important than ever to step back and evaluate the design, operation and effectiveness of your company's compliance program. With the heightened expectations raised by the guidance, and the increasing complexity of risks facing insurers, it is appropriate to consider how your company is positioned now and going forward.

Contacts

George Hanley
Managing Director | Deloitte & Touche LLP
ghanley@deloitte.com

Tim Cercelle
Managing Director | Deloitte & Touche LLP
tcercelle@deloitte.com

Mike Ruiz
Senior Manager | Deloitte & Touche LLP
miruiz@deloitte.com

Carolyn Mellett
Senior Manager | Deloitte & Touche LLP
cmellett@deloitte.com

John Bannon
Consultant | Deloitte & Touche LLP
jbannon@deloitte.com