

4 Ways To Improve Your Compliance Program In 2023

By **John Kocoras and Joseph Yaffe** (January 2, 2023)

The fundamental components of effective corporate compliance programs have not changed significantly in recent years.[1] However, U.S. enforcement authorities are trying to reinvigorate companies' attention to those programs.

U.S. Department of Justice leaders expressed particular concern in 2022 about whether companies have appropriately integrated their compliance departments.

In March, Assistant Attorney General for the DOJ's Criminal Division Kenneth Polite Jr. — a former corporate chief compliance officer — described his perception of compliance professionals' environments at New York University Law School's program on corporate compliance and enforcement: "I know the resource challenges. The challenges you have accessing data. The relationship challenges. The silo-ing of your function."

He warned companies: "Support your compliance team now or pay later." [2]

U.S. Deputy Attorney General Lisa Monaco repeated these concerns in September, explaining that "resourcing a compliance department is not enough; it must also be backed by, and integrated into, a corporate culture that rejects wrongdoing for the sake of profit." [3]

The remarks accompanied her release of a memorandum that federal prosecutors must follow when evaluating the strength of a company's compliance program in determining how to resolve an investigation.[4] The memorandum challenges companies to ensure that compliance programs have the highest levels of company attention, are resourced appropriately and do not operate in silos.[5]

Improving integration should be near the top of many companies' compliance program goals for 2023. Summarized below are four actions companies should consider completing next year to help ensure that their compliance programs are optimized and effectively positioned to respond to government review.

This is of course not an exhaustive list of aspects of compliance programs that warrant attention, but rather suggestions on elements that would likely benefit from a fresh look.

Compensation Agreements and Incentives

Companies should review compensation agreements and incentives with senior leadership, business team leaders, sales professionals, third-party agents and possibly others to ensure structures promote compliance and define consequences for misconduct.

This likely will require collaboration among compliance, legal and human resources professionals, along with business team leaders and the company's compensation committee.



John Kocoras



Joseph Yaffe

The U.S. deputy attorney general's memorandum provides the DOJ's first formal guidance on evaluating companies' compensation plans and agreements in connection with resolutions of criminal investigations.

The most significant plans and agreements for compliance purposes are likely to involve senior executives responsible for leading functions and the company's tone at the top; sales team leaders and sales professionals including third-party agents whose compensation might be influenced by sales volume; and professionals who routinely communicate with government officials, including employees of state-owned enterprises.

The U.S. deputy attorney general recommends that when evaluating a company's compliance program, prosecutors should consider whether the company's compensation arrangement, plans and agreements provide for penalties — including in the form of clawback rights — that may be levied against current or former employees, and directors whose actions or omissions contributed to criminal conduct.

Notably, such clawback rights would exceed requirements in newly finalized clawback rules under the Dodd-Frank Wall Street Reform and Consumer Protection Act. The Dodd-Frank clawback rules mandate clawback policies for publicly traded companies in the event of financial restatements but do not require clawback solely as a result of misconduct or criminal activity.

Presumably, the presence and application of more traditional concepts of compensatory penalties in the event of termination of employment for "cause," where cause is defined to include violations of criminal law, would be viewed favorably by prosecutors. Additional guidance from the DOJ's Criminal Division on how to reward companies that implement and apply compensation clawback policies is expected to be forthcoming.

The U.S. deputy attorney general's memorandum also encourages the promotion of ethical corporate culture by rewarding, via financial incentives, compliance within an organization. The examples provided include the use of compliance metrics and benchmarking in setting incentive targets as well as performance reviews that take into consideration compliance-promoting behavior.

Compliance program agendas for 2023 should include assessments of compensation arrangements to understand what recourse, if any, companies have against individuals' past or future compensation in the event of criminal misconduct. Revisions or additions to existing arrangements may require employee consent and/or adjustments to compensation program design.

Any revisions will need to consider the impact of, or limitations under, applicable local laws and regulations including applicable non-U.S. laws and regulations.

In considering whether to make revisions to their compensation programs, companies may find it effective to integrate the compliance department into the compensation design workflow.

Finally, compensation committees tasked with designing and implementing senior executive compensation plans should consider whether and to what extent their programs may be well-served by creating additional incentives for compliant behavior.

Corporate Documents

Compliance should assess how quickly their legal and compliance personnel can collect corporate documents, including emails and text messages, originating or maintained in locations where the company operates. This likely will require participation by information security leadership, local office leadership and finance team members, along with legal and compliance staff.

Companies' information systems and employees' methods of communicating with each other and with outsiders are constantly evolving.

In order to meet enforcement authorities' expectations, companies must know in advance how best to access company communications and other data essential to a thorough investigation of any allegation of misconduct.

Compliance departments should work with other functions to identify potential technological barriers to collection, including employees using their own devices and communications apps with end-to-end encryption.

Laws affecting a company's ability to gather and transmit communications and other data essential to understanding whether misconduct occurred can vary widely across the locations where the company operates.[6] Companies should know in advance how feasible it will be, both logistically and legally, to gather materials from its various offices quickly following an allegation of misconduct or a subpoena.

This might require approaches tailored to specific laws such as the European Union's General Data Protection Regulation and China's Personal Information Protection Law, as well as the companies' information systems.[7]

Considering the constant change in communication methods and privacy laws, this assessment should occur not only in 2023, but on at least an annual basis afterwards.

While companies can never ensure that they will have complete access to all written communications relevant to an investigation, they will be far better off after identifying possible gaps and establishing policies and procedures to minimize those gaps.

Success Stories

Companies should compile a list of their compliance success stories, with input from personnel on the compliance, legal, human resources and internal audit teams.

The U.S. deputy attorney general's memorandum instructs that companies "should be prepared to produce a list and summary of all prior criminal resolutions within the last ten years and all civil or regulatory resolutions within the last five years," as well as any known pending government investigations.[8]

For most companies, that information will be readily available and not extensive. Authorities are not limited, however, to considering only criminal, civil or regulatory resolutions or pending government investigations when addressing a new matter.

Companies undoubtedly will have successfully addressed compliance concerns in prior years that never resulted in a formal resolution or government investigation.

A list of these successes is best prepared before a company is facing investigation and updated periodically. The list could be useful in demonstrating a commitment to compliance,

provided that the matters did not rise to the level that authorities would have expected to be self-disclosed, or were in fact self-disclosed.

Basic examples include decisions to terminate a vendor or to cancel a planned acquisition where the company could not get sufficient assurances that its compliance policies would be strictly followed. Collaboration across functions will often be necessary to make sure that knowledge of key successes is not siloed within the company.

Due Diligence in Acquisitions

Companies should revisit due diligence processes to ensure they include evaluating prospects for successfully integrating a new business into the existing compliance program. This will require guidance from the compliance and legal departments with input from business team leadership, finance and information security.

Fears of successor liability based on a target company's dated misconduct can doom an acquisition, even if the acquisition would promote anticorruption goals by placing a company with compliance challenges into a company with a robust compliance program.

The U.S. deputy attorney general's memorandum reinforces that federal prosecutors will continue to take a tough stance on historical misconduct that occurred at an acquired company.

It states that misconduct at an acquired company should merely receive "less weight" in prosecutors' evaluation of a potential resolution of a current investigation of the acquiring company if the acquired company has been "integrated into an effective, well-designed compliance program," the acquirer had "addressed the root cause" of the misconduct at the acquired company before the current investigation, and "full and timely remediation occurred within the acquired entity" before the investigation.[9]

Companies must continue to assess not only whether an acquisition target engaged in unlawful activity, but how effectively the target's personnel will adapt to a new, robust compliance program in order to meet this high bar. Obstacles to that integration could significantly reduce or eliminate the benefits of the acquisition.

The compliance department plays an important role in identifying risks and defining expectations, but other functions in the acquiring company likely will be in a better position to evaluate the prospects for a successful integration into a compliance program.

Conclusion

John F. Kennedy famously declared 60 years ago that "the time to repair the roof is when the sun is shining." Prioritizing compliance program integration in 2023 will be helpful not only when storm clouds roll in, but it could help keep them away altogether.

John C. Kocoras is a partner at Skadden Arps Slate Meagher & Flom LLP. He formerly served as first assistant U.S. attorney in the U.S. Attorney's Office for the Northern District of Illinois.

Joseph M. Yaffe is a partner at Skadden.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] See, e.g., U.S. Sent'g Guidelines Manual § 8B2.1; U.S. Department of Justice Criminal Division, "Evaluation of Corporate Compliance Programs" (updated June 2020).

[2] See Assistant Attorney General Kenneth A. Polite Jr., Remarks at New York University Law School's Program on Corporate Compliance and Enforcement, March 25, 2022.

[3] See U.S. Deputy Attorney General Lisa O. Monaco, Remarks on Corporate Criminal Enforcement, Sept. 15, 2022.

[4] See memorandum from U. S. Deputy Attorney General Lisa Monaco (Sept. 15, 2022).

[5] See our October 6, 2022, client alert "Revisions to the DOJ's Corporate Criminal Enforcement Policy Will Require Companies To Reevaluate Their Compliance Systems."

[6] See our September 21, 2022 client alert "Recent Trends in China-Related Cross-Border Enforcement."

[7] See our November 3, 2021, client alert "China's New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies."

[8] See memorandum from Deputy Attorney General Lisa Monaco, p. 5, fn. 5 (Sept. 15, 2022).

[9] See memorandum from U.S. Deputy Attorney General Lisa Monaco, pp. 5-6 (Sept. 15, 2022).