The United States Law Week

INSIGHT: Crisis-Proofing Your Compliance Program—Five Key Questions

By Jennifer Saperstein, Benjamin Haley, and Sarah Crowder

April 27, 2020

Covington attorneys say companies should ask themselves five key questions about their compliance programs to ensure they are ready to face any crises—including the coronavirus pandemic—and be ready for current and future business disruptions.

The Covid-19 pandemic and responses, including social distancing and stay-at-home orders, bring to the forefront numerous challenges for compliance programs that rely on face-to-face contact and getting compliance professionals on the ground in business operations.

Companies facing these challenges should consider how effectively their programs function during crises.

Below are five questions companies should ask to help "crisis-proof" compliance programs for Covid-19, natural disasters, and other significant business disruptions.

1. Have You Assessed Compliance Risks Posed by Crises?

Covid-19 has placed immense financial and operational pressures on businesses. Meanwhile, governments face unprecedented challenges managing their responses, supply chains are disrupted, and companies have rapidly transitioned to remote working. These pressures and challenges can increase compliance risks on numerous fronts.

For example:

- Government processes (e.g., licenses and permits, customs clearances)—which present compliance risks in the best of times—are subject to increased strain, or worse, not functioning at all. This increases administrative bottlenecks, leading to operational pressures and increased corruption risks. Uncertainty about the application and scope of stay-at-home or lockdown regulations leaves government officials with increased discretion and may present temptations to seek improper benefits.
- Significant supply chain disruptions may cause companies to consider new business partners or restructure existing arrangements. At the same time, companies may explore more frequent or larger donations of goods or services. Compliance personnel may find themselves under pressure to deviate from or significantly expedite existing due diligence and other compliance procedures.
- Personnel operating under increased pressures may be more inclined to make questionable ethical decisions to generate business or simply "get things done."

Assessing the immediate compliance risks posed by Covid-19 and business recovery efforts, and taking appropriate mitigation steps, is critical. This type of risk assessment need not be as formal and structured as periodic risk assessments undertaken in the normal course of business.

For example, one way to proceed is to conduct regular check-ins with key business leaders involved in the company's crisis management efforts, exploring the types of government interactions and challenges they are facing, and associated compliance risks.

2. Do You Have the Right Resourcing and Structure?

In times of crisis, important decisions are made quickly and under stress. A heightened emphasis on critical business priorities risks pushing compliance down the priority list, and it may prove more difficult for compliance personnel to engage management and employees. Ideally, compliance professionals will have a seat at the table with business leaders so they can spot and address compliance risks as new business strategies and solutions are discussed.

While crisis situations may not be the optimal time to realign reporting lines or increase headcount, companies should assess whether compliance personnel are represented on crisis management teams, compliance resources can easily and immediately be deployed across the organization, and employees outside of the compliance function can be “deputized” to carry out compliance responsibilities.

3. Do You Have a Crisis Management Plan?

Companies should be prepared for the reality that crises like Covid-19 will disrupt normal compliance program operations, particularly those relying on in-person interaction. Compliance functions should consider developing crisis management plans to ensure program continuity, looking to best practices from other company functions more experienced with such plans, such as corporate security.

While the substance of a crisis management plan should emerge through an assessment of how compliance processes might be disrupted and the steps necessary to mitigate disruptions, in all circumstances such a plan should address communication protocols. For example, it may address issues such as how compliance functions can remain visible, ensuring that employees are aware of compliance resources and reinforcing the company’s commitment to compliance.

There may be pressure to cancel or delay certain proactive compliance activities such as risk assessments, trainings, or audits so that the business can focus on responding to a crisis. A crisis management plan can help compliance teams make risk-based decisions on which activities reasonably can be delayed while ensuring that pressing risks are addressed. Crisis management plans may also address ways to expedite or adjust key compliance processes—such as third party due diligence—to the extent necessary, without raising unacceptable risks.

4. Are You Effectively Leveraging Technology?

With businesses transitioning to remote working, many compliance professionals have quickly adjusted to conducting work that is typically done in person (e.g., witness interviews) by video or audio conference. This poses challenges, particularly with document-intensive interviews, and companies should consider technology investments that enable high-quality interactions and secure content sharing.

Companies should also consider how ordinary course compliance consults and reporting may be affected if employees are not interacting in person. For example, companies may consider increased use of electronic portals or mobile apps through which employees can seek compliance advice.

If companies experience decreased reporting of compliance incidents, they should consider whether this results from decreased commercial activity or limitations in their reporting channels.

Finally, companies can consider investment in technology solutions (e.g., data analytics platforms) to enable compliance monitoring without being physically present. In addition to enabling companies to better detect and prevent corrupt payments, such systems can help catch fraud and embezzlement, which often increase in times of economic stress.

5. Are You Continually Assessing if Your Program is Crisis-Resilient?

Compliance professionals are intimately familiar with the notion that their programs should not be static, but should evolve with changes in the company's business. With this concept of continuous improvement in mind, it is wise to consider how resilient their programs are to crises.

For example, just as companies consider how effective their programs are in meeting the challenges of expansion into new markets or business lines, they can seek to assess how effectively their programs have responded to the challenges of Covid-19 and other crises, and make enhancements in light of lessons learned. This need not be a standalone exercise, but rather can be accomplished through targeted lines of inquiry in a company's ordinary course efforts to assess the effectiveness of its program.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

Author Information

Jennifer Saperstein, vice chair of Covington's Anti-Corruption Practice Group, is an experienced compliance counselor. She conducts risk and compliance program assessments, and develops compliance programs across a range of industries.

Benjamin Haley leads Covington's compliance and investigations practice in Africa. He advises clients on a wide range of risk and compliance matters, including M&A transactions, risk and program assessments, and data analytics.

Sarah Crowder is special counsel at Covington in London and has a broad compliance and investigations practice. She helps clients in various industries develop compliance programs, conduct risk assessments, conduct transactional and third-party due diligence, navigate post-acquisition compliance integration projects, and deliver compliance training.