Remediation Assessment Framework

The Government stresses the importance of remedial measures and other procedures to prevent further recurrence of misconduct in determining whether to file criminal charges or enforcement proceedings, impose a monitor, and seek fines and other penalties. The Government, however, provides no detailed guidance for prosecutors, regulators, compliance officers and counsel on the criteria they should consider and the procedures they should perform to assess the effectiveness of the remediation and other corrective measures.

StoneTurn Group's assessment sets forth key criteria, which we draw from the DOJ, *Principles of Federal Prosecution of Business Organizations* (2008); SEC, Enforcement Division, *Enforcement Manual* (2012); DOJ and SEC, *Resource Guide to the U.S. Foreign Corrupt Practices Act* (2012); *U.S. Sentencing Guidelines, Chapter 8* (2012); FINRA, *Sanction Guidelines* (2011); Committee of Sponsoring Organizations (COSO) of the Treadway Commission, *Internal Control – Integrated Framework* (2013); and DOJ and SEC settlement agreements.

For detailed procedures and guidance on conducting these assessments, please contact:

Jonny Frank
+1 212 430 3434
jfrank@stoneturn.com

TIMELINESS	TEAM COMPETENCE	INDEPENDENCE	ROOT CAUSE ANALYSIS	OTHER MISCONDUCT
Did the organization…				
Commence remediation promptly after discovery of misconduct?	Include experts in risks, controls, forensic analytics and audit on its remediation team?	Engage an outside professional adviser as recommended by the U.S. Sentencing Guidelines?	Employ a structured process to conduct an analysis of why and how the misconduct occurred?	Conduct audit procedures to detect other misconduct by the perpetrator(s)?
Actually implement steps to prevent recurrence or just state that it will take future steps to implement?	Seek experts in prevention and detection, and not just investigation?	Independently assess and audit the remediation program?	Use a risk assessment to identify risks? How did flawed incentives and corporate culture contribute?	Conduct audit procedures to detect similar misconduct by others in the organization?

DISCIPLINARY MEASURES	PROCESSES & CONTROLS	RESTITUTION	SELF-REPORTING	ASSESSMENT & AUDIT
Did the organization…				
Employ a fair and consistent disciplinary process? (e.g., Did high producers or senior personnel receive special dispensation?)	Implement new or enhanced processes and controls to prevent and timely detect recurrence of similar misconduct?	Take appropriate steps to quantify the loss, and identify, notify and make full restitution to the victims?	Consider (on the advice of counsel) whether to self-report misconduct to the authorities?	Engage an independent, third party to assess the remediation process and implementation of corrective measures?
Take appropriate disciplinary measures for failing to prevent, detect and report misconduct?	Consider the use of forensic analytics and other technology tools to prevent recurrence?	Make restitution voluntarily or was it court-ordered?	Self-report voluntarily or was it required to do so by rules or regulations?	Periodically audit the new and enhanced processes and controls?

STONETURN GROUP

www.stoneturn.com

5 Ways To Meet DOJ's Heightened Compliance Expectations

Jonny Frank

LAW360.COM

With billion-dollar penalties for misconduct almost becoming commonplace, it's no surprise the U.S. Department of Justice is raising the bar for compliance risk assessments — or that companies must focus more on identifying risks before they become issues.

At a recent conference of compliance officers, assistant attorney general for the Criminal Division, Leslie Caldwell, took aim at the compliance risk assessment process, commenting, "[C]ompliance programs are too often behind the curve, effectively guarding against yesterday's corporate problem but failing to identify and prevent tomorrow's scandals."[1]

> "COMPANIES FOCUSED SOLELY ON REGULATORY RISK OFTEN OVERLOOK OTHER SIGNIFICANT RISKS THAT CAN POSE CRIMINAL OR CIVIL LIABILITY."

When confronted with misconduct, counsel and compliance officers need to be prepared to answer whether the company had identified the violation as a potential risk. If the answer is no, the company must justify "why not;" and, if yes, explain why pre-incident policies and controls failed to prevent the misconduct.

Here are five practical ways to meet heightened expectations:

1. Regulatory Risk ≠ Compliance Risk

Caldwell aptly noted that compliance risk assessments need to reach beyond regulatory risk. Some companies, particularly those in regulated industries, differentiate between regulatory and compliance requirements — the former referring to specific industry regulations, and the latter referring to general legal requirements.

Compliance risk falls generally into four areas: **(1)** federal, state, local and foreign law; **(2)** industry-specific regulations; **(3)** contractual requirements; and **(4)** compliance with internal company policies. Companies focused solely on regulatory risk often overlook other significant risks that can pose criminal or civil liability, create financial loss, or damage reputation and important relationships.

2. COSO Integrated Internal Controls and Enterprise Risk Frameworks

When it comes to evaluating ethics and compliance programs, lawyers and compliance officers typically rely on the criteria in the U.S. Sentencing Guidelines, Chapter 8 Sentencing of Organizations (USSG).[2] Auditors prefer the standards issued by the Committee of Sponsoring Organizations of the Treadway Commission, referred to simply as COSO.[3] COSO is the leading risk management framework and the standard upon which most public companies base their Sarbanes-Oxley assertion to the effectiveness of financial reporting controls.

Although the USSG speaks to assessing risk, it provides little direction on how to perform risk assessments. But COSO provides guidance.

At the risk of oversimplification, COSO defines "risk" as any event that impedes an organization to achieve its operational, reporting, strategic or compliance objectives. In doing so, COSO relies on schemes and scenarios. Take, for example, payments to public officials. Many lawyers would generally describe this as Foreign Corrupt Practices Act risk. Under the COSO approach, the organization enumerates potential schemes and scenarios by which the payments might be made. Input from forensic risks experts and experienced white collar lawyers is essential to this process, as they are in the best position to understand how such schemes are perpetrated within the context of the industry in which the company operates, its business model and its relationships.

3. Assessing Significance

A compliance risk assessment generally begins with identifying inherent risk, that is, without regard to mitigating controls. (Residual risk refers to the risk after taking mitigating controls into account). Inherent risk protects the risk assessment team from relying upon ineffective controls.

Next, the team measures significance to weed out inconsequential risks. It is at this step that companies encounter trouble. Noting that "corporations all too often misdirect their focus to the wrong type of risk," Caldwell explained that the DOJ has "repeatedly seen corporations target the risk of regulatory or law enforcement exposure of institutional and employee misconduct, rather than the risk of the misconduct itself."[4]

Stated differently, we often see companies measure significance by attempting to quantify the likely direct monetary penalty if they get caught. This approach is akin to assessing the significance of drunk driving to the likely penalty in the event of a police stop. Instead, companies should holistically assess significance, including the impact on potential victims, brand and reputation, and relationship with customers, suppliers, employees, etc.

Counsel and compliance officers serve an essential role. Companies often defer assessment to the business unit and functions leaders impacted by the risk. Business leaders, however, are not — and should not be — compliance experts. Their focus should be on improving and achieving operational efficiency. In doing so, however, they are vulnerable to missing the bigger picture, particularly, if the company measures them on profit and loss.

4. Overreliance and Underutilization of Other Risk Assessments

Companies perform all types of risk assessments. Internal audit assesses risk when developing its annual audit plan. Enterprise risk assessment identifies catastrophic risk. Operational risk assessment focuses on financial impact. Individual business units and functions commonly perform risk assessments to develop financial forecast and budgeting.

On their own, none of these factors qualify and it would be a mistake to rely upon them as a compliance risk assessment. That does not mean, however, that these assessments are unsuitable for a compliance risk assessment. Done properly, and with the inclusion of individuals knowledgeable about and skilled in compliance, the company and the industry in particular, they provide an opportunity to assess compliance risk without conducting a separate compliance risk assessment.

5. Document, Document, Document

Effective defense of the company's compliance risk assessment process — whether it be to the board compliance committee or prosecutors and regulators — demands contemporaneous, written documentation. Verbal reconstruction of the assessment will not suffice. A variety of formats are available, although, most companies employ a simple Excel worksheet to track: **(1)** inherent risk; **(2)** impacted business units and functions; **(3)** reason for inclusion; **(4)** assessment of inherent significance and likelihood; **(5)** description of organization's risk response; **(6)** summary of procedures to evaluate design and validate operating effectiveness; and **(7)** a summary of additional planned procedures, if any.

Conclusion

Risk assessments form the cornerstone of an effective compliance program. If the five measures outlined above are implemented effectively and documented contemporaneously, a company stands a good chance of passing a post-incident prosecutorial assessment of its pre-incident compliance program.[5] Compliance risk assessments conducted poorly — or worse, not at all — can likely lead to criminal prosecution, enhanced fines and penalties, and possible imposition of a government compliance monitor.

To learn more, visit www.stoneturn.com
Follow us on LinkedIn.

[1] DOJ, Assistant Attorney General Leslie R. Caldwell Remarks at the Compliance Week Conference (May 2015) ("Caldwell Remarks") available at www. http://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-compliance-week-conference.

[2] United States Sentencing Commission Guidelines Manual, Ch. 8 (2014)

[3] COSO is a not-for-profit joint initiative of the American Accounting Association, American Institute of CPAs, Financial Executives International, the Association of Accountants and Financial Executives in Business, and the Institute of Internal Auditors. Its stated mission is to develop "comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations." More information can be found at: www.coso.org.

[4] Caldwell Remarks, supra.

[5] See U.S. Attorneys' Manual 9-28.300, Principles of Federal Prosecution of Business Organizations U.S. DOJ, Principles of Federal Prosecution of Business Organizations (2011) (requiring federal prosecutors to consider "existence and effectiveness of the corporation's pre-existing compliance program") available at http://www.justice.gov/usam/usam-9-27000-principles-federal-prosecution); District Attorney of the County of New York, Considerations in Charging Organizations (2010) (requiring prosecutors to consider "the organization's previous efforts to address corruptive influences by means of compliance programs") available at http://manhattanda.org/sites/default/files/Considerations%20in%20Charging%20Organizations.pdf.