

“Pre-Incident” Compliance Program Assessment Framework

Prosecutors and regulators must assess the effectiveness of an organization’s “pre-existing” compliance program to determine 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 conduct to assess the effectiveness of the compliance program at the time of the violation.

StoneTurn Group’s assessment of the existing compliance program will draw key criteria from a variety of relevant authoritative literature including but not limited to 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

CONTROL ENVIRONMENT	RISK ASSESSMENT	CONTROL ACTIVITIES	INFORMATION & COMMUNICATION	AUDIT & MONITORING
Did the organization...				
Promote a culture that encourages ethics and compliance with the law? Did it demonstrate a commitment to a culture of compliance?	Use a risk assessment as a fundamental component of the compliance program, and periodically assess and document risk of misconduct?	Promulgate visible and clear policies, standards and procedures?	Communicate policies effectively to directors, employees, joint venture partners, agents, suppliers, and other relevant third parties?	Review its ethics and compliance standards and procedures no less than annually?
Assign effective oversight and day-to-day responsibility over the compliance program? Did it provide adequate resources and direct Board access?	Implement an ongoing risk assessment, and update the assessment with company and industry developments?	Have controls to ensure fair and accurate books, records and accounts?	Provide adequate training, including annual certifications, and a resource to provide advice?	Equip audit and operational personnel with adequate detection tools and training?
Have an incident response process? Did the process provide for taking steps to remedy harm and avoid future misconduct? Did the organization take those steps?	Identify the violation as a risk? If not, why?	Have controls to ensure that assets could not be acquired, used or disposed to commit or conceal misconduct?	Make adequate use of technology including forensic data analytics and security systems?	Conduct forensic audit procedures to detect misconduct, including the identified misconduct?
Assess how the corporate culture and control environment impacted the occurrence and detection of the misconduct?	Look at how the risk process impacted the occurrence and detection of the misconduct?	Examine how the policies, procedures and controls impacted the occurrence and detection of the misconduct?	Evaluate how information and communication issues impacted the occurrence and detection of the misconduct?	Look at how the audit and monitoring impacted the occurrence and detection of the misconduct?

STONETURN
GROUP

www.stoneturn.com