

Ethics & Compliance Assessment Framework

Does your organization meet expectations and maximize benefits of ethics and compliance programs? The DOJ has observed that “compliance programs are too often behind the curve, effectively guarding against yesterday’s corporate problem but failing to identify and prevent tomorrow’s scandals.” Effective ethics and compliance programs more than pay for themselves through enhanced operational effectiveness, and safeguard brand value and the personal reputations of the board and management.

StoneTurn Group’s assessment of the ethics and compliance programs draws government pronouncements and various 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); and Committee of Sponsoring Organizations (COSO) of the Treadway Commission, *Internal Control – Integrated Framework* (2013).

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

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

CONTROL ENVIRONMENT	RISK ASSESSMENT	CONTROL ACTIVITIES	INFORMATION & COMMUNICATION	AUDIT & MONITORING
Does the organization...				
Promote a culture that encourages ethics and compliance? Do senior leaders provide strong, explicit and visible support for corporate compliance? Does the organization tacitly encourage misconduct to achieve business objectives?	Identify and assess ethics and compliance risk? Does the assessment process extend to risks of unethical conduct and non-compliance with: (1) federal, state, local and foreign laws; (2) industry specific regulations; (3) internal policies; and (4) contractual obligations?	Promulgate visible and easily understood policies? Does the organization enforce policies through disincentives / discipline and stress compliance through in-person meetings, e-mails and telephone calls?	Communicate policies effectively to directors, employees, joint venture partners, agents, suppliers, and other relevant third parties?	Review ethics and compliance standards and procedures no less than annually? Does the review evaluate the design and operating effectiveness of the control environment, risk assessment, compliance controls, information technology, and monitoring?
Assign oversight and day-to-day responsibility over the compliance program to senior executives who report directly to independent monitoring bodies – for example, internal auditors or the board of directors?	Employ a recognized process such as the COSO Integrated Internal Controls Framework? Does the risk assessment include unit and function leaders and require acknowledgement of responsibility?	Assess whether policies, procedures and controls can be circumvented through management override, collusion or other means? Does the organization audit operating effectiveness of compliance processes and controls?	Provide adequate training, including annual certifications, and a resource to provide advice?	Equip audit and operational personnel with specialized training, tools and, if needed, expert resources to audit compliance controls? Does the review rate deficiencies and require corrective measures?
Provide adequate funding and access to necessary resources for the ethics and compliance functions? Do they carry appropriate stature in the organization?	Keep up-to-date with evolving organization and industry risks and circumstances, including when the organization merges with or acquires another organization?	Maintain controls and accurate books, records and accounts, and ensure assets cannot be acquired, used or disposed of to commit or conceal misconduct?	Make adequate use of technology, including forensic data analytics and security systems?	Develop risk factors and indicators, and employ forensic data mining and other procedures to detect misconduct in the absence of an allegation or suspicion?
Have a process – with sufficient resources – for investigating and documenting alleged and suspected misconduct? Does the process provide for remediation? (N.B.: See StoneTurn’s Remediation and Pre-Compliance Program Assessment Frameworks)	Integrate compliance risk assessment with other risk assessments (e.g., annual internal audit planning and annual budgeting)? Does the organization document risk assessment processes and results?	Sensitize third parties (e.g., vendors and agents) to the importance of clients, including more than boilerplate contract language and termination of business relationships for non-compliance with laws and policies?	Evaluate how information and communication issues impacted the occurrence and detection of the misconduct?	Document the ongoing monitoring of the ethics and compliance program? Does the organization contemporaneously take credit for positive actions to later defend its efforts and the program?

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 and other 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?