LEAVING NO STONE UNTURNED:
Meeting SEC and FINRA Expectations

April 2013

Meeting SEC and FINRA Expectations about Remediation

By Jonny Frank, StoneTurn Group LLP

Both the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) stress the importance of remediation. The SEC's Division of Enforcement Manual cites remediation as one of four factors to consider in deciding whether, and to what extent, a company deserves credit for cooperation. The United States Department of Justice (DOJ) and SEC Resource Guide to the U.S. Foreign Corrupt Practices Act (Resource Guide) places a "high premium" on remediation in resolution of cases and is a key factor in deciding whether to impose an independent corporate monitor. Similarly, FINRA Regulatory Notice 08-70 (FINRA Reg. 08-70) instructs that timely and effective remediation is one of four factors that FINRA considers in awarding credit for "extraordinary cooperation." FINRA Sanction Guidelines explain that disciplinary sanctions are "remedial in nature and should be designed to deter future misconduct."

It is not just the organization that is impacted by issues arising from poor internal controls. Board members and senior management face substantial embarrassment and damaged personal reputation. Consider also the career damage to business leaders, ethics and compliance officers, and internal auditors who must report that the organization has been victimized or engaged in misconduct.

The bright side is that remediation is good for business. According to a survey conducted by the Economist Intelligence Unit, companies lose, on average, 2 percent of earnings or the equivalent of one week's revenue to fraud; 18 percent lose two weeks or more of revenue. These estimates do not include waste, abuse, fines, investigative and legal fees, or higher insurance premiums. Nor do they capture "soft" costs—management distraction, lost productivity, talent flight, injured customer and supplier relationships, opportunity loss, and erosion of brand value. The Association of Certified Fraud Examiners' *Report to the Nations* finds that effective antifraud programs cut losses in half, saving most organizations millions of dollars in future losses.

Neither the SEC nor FINRA provide guidance about what constitutes effective remediation. The following are key elements as cobbled from SEC and FINRA settlement agreements, the DOJ, and the United States Sentencing Commission criteria and risk management principles.

Timeliness

Government expectations are clear: start remediation efforts early. Do not wait until the investigation is complete. It is one thing to assert that the organization will take steps to prevent recurrence; it is quite another to prove that those steps have been identified, considered, and implemented—albeit preliminarily—as the investigation progresses.

Both the SEC and FINRA consider the timeliness of the remediation in determining what charges to file and remedies to seek. FINRA Reg. 08-70 credits post-detection remediation only if "taken early on, well before completion of FINRA's investigation" and awards no credit for remedial measures taken "later in the investigation." Just recently, for example, Morgan Lewis & Bockius successfully obtained "extraordinary cooperation" credit and a substantially reduced fine for its client, HSBC Securities (USA) Inc. (HSI) based largely on timely and effective remediation for multiple violations that occurred over several years. FINRA noted that HSBC Securities "remediated its systems, procedures, and controls to prevent future violations in each of these areas—all prior to FINRA's involvement. Moreover, HSI took the additional step of verifying that its remediation efforts were fully effective."

The Resource Guide explains that swift remediation is essential to avoid imposition of a monitor or independent consultant. Timely remediation substantially reduces penalties, potentially saving millions of dollars in fines and penalties.

Independence and Privilege

If the allegations warrant an independent third-party investigation, they likely also merit independent third-party remediation. Independence also poses an issue when evaluating the effectiveness of remedial measures. The evaluator must be independent from the remediation team, particularly if the organization seeks to impress the government. Internal Audit Standards, for example, would prohibit internal audit to conduct the assessment if it participated in developing and implementing remedial measures.

Companies should remediate, if possible, under the attorney client privilege, as the process may unearth other misconduct. The organization eventually will need to waive privilege to report remedial measures to regulators. Consider forming two attorney-led work streams: one for investigation and another for remediation. Separate teams ensure proper allocation of skill sets and avoid the remediation delays that invariably occur from the investigation team being too busy to focus on remediation. Coordination between the teams is essential and best achieved if the remediation team communicates processes and results to the lawyer heading the investigation team.

Forensic Risks and Controls Expertise

Forensic Risks & Controls (FR&C) is a different discipline than forensic accounting. FR&C experts work in the absence of a specific allegation or suspicion. Forensic accounting, in contrast, helps clients prove or disprove allegations.

FR&C experts are knowledgeable in frameworks for identifying and managing risks and experienced in conducting risk assessments, assessing the control environment, evaluating design and operating effectiveness of preventive and detective internal controls, developing forensic data analytics, and conducting forensic audits. The 2011 amendments to the United States Sentencing Guidelines (USSG) acknowledge this difference in expertise and specifically recommend inclusion of FR&C experts on the remediation team. Select a remediation advisor experienced in working and coordinating with legal teams; legal crises are not the time to learn the subtleties of the attorney-client privilege and work product doctrine. The remediation expert should also have on-the-ground experience relating to preventing and detecting fraud and corruption. These matters raise unique issues and challenges in developing transaction-level control activities, key risk factors and indicators, data analytics, and monitoring and auditing.

Root Cause Analysis

Remediation addresses "why" and "how" just as investigation determines "who," "what," and "when." The "Cressey fraud triangle," named after 1950s criminologist Donald Cressey, is a useful framework for root cause analysis in simple and insignificant matters. According to Cressey, three conditions exist whenever misconduct occurs: (1) incentive or pressure, (2) opportunity, and (3) rationalization. The analysis thus considers the perpetrators' motivation, their justification for their misconduct: control gaps.

Complex or significant misconduct warrants deeper analysis. My firm suggests the Committee of Sponsoring Organization of the Treadway Commission (COSO) framework, recognized globally as the leading risk-management and controls framework and expressly approved by the SEC. Public companies universally apply COSO to meet Sarbanes-Oxley Act requirements regarding controls over financial reporting. COSO is equally applicable to operation and compliance risks and controls.

COSO entails an analysis of the control environment, risk assessment, control activities, information and communication, and monitoring. These elements correspond to USSG Chapter 8 criteria of an effective ethics and compliance program. The USSG, of course, is United States-centric and designed for criminal proceedings. COSO is a universal standard. The elements are as follows:

> *Control environment.* This refers to corporate culture, which includes commitment to integrity, "tone at the top," codes of ethics and conduct, mechanisms to report misconduct, training, and so on. The root cause analysis should consider whether and how the control environment may have contributed to the underlying misconduct.
>
> *Risk assessment.* Risk assessment is the cornerstone of an effective antifraud and ethics and compliance program. A proper root cause analysis considers whether the organization identified the risk and, if so, linked and evaluated the response. Remediation must correct weaknesses or deficiencies in the risk-assessment process to ensure that the organization properly anticipates and addresses future risks.
>
> *Control activities.* Control activities refer to preventive and detective transaction-level controls and "design" and "operating" effectiveness. Serious misconduct almost always involves flawed internal control activities. Root cause analysis determines whether the flaw(s) are of design effectiveness, operating effectiveness, or both.
>
> *Information and communication.* Information and communication refers to the information systems existing within an organization and how these systems communicate with one another. This element also considers how the organization leverages (or fails to leverage) forensic data analytics and security systems to prevent and detect misconduct in a timely manner.
>
> *Monitoring and auditing.* Monitoring and auditing includes contemporaneous and after-the-fact reviews to detect key fraud "risk factors" and "risk indicators" and to identify whether the controls are effective in addressing them. Risk factors are circumstances that impact likelihood of a fraud occurring. Risk indicators are red flags that the misconduct exists. The root cause analysis should consider the quality of the company's monitoring and auditing systems and whether the misconduct was detected in a timely manner.

Other Misconduct

Companies must flush out other misconduct by the perpetrators and similar misconduct by others in the organization. Imagine the embarrassment and possible legal consequences if the company or government subsequently discovers that the perpetrators engaged in other wrongdoing or, perhaps worse, that the misconduct claimed to be remote actually pervades the organization. The remediation team gains comfort through an auditing process called "negative assurance," which means conducting audit procedures to search for risk indicators.

> *Perpetrator misconduct.* Do not be fooled by tears or expressions of regret; perpetrators rarely come completely clean. Apply COSO risk-assessment procedures to identify other ways that the perpetrators may have engaged in misconduct.
>
> *Misconduct by others.* Use the root cause analysis to gain assurance that similar misconduct has not occurred elsewhere in the organization. Consider both design and operating effectiveness. If the misconduct arose from poor operating effectiveness, test whether control activities are operating effectively in a sample of other locations. If the design is flawed, the team might need to conduct substantive forensic audit procedures to search for red flags of similar misconduct.

Entity- and Transaction-Level Internal Controls

Entity-level internal controls refer to controls that apply across the organization and reinforce the control environment (e.g., codes of conduct, training, and whistleblower training). *Transaction-level internal controls* refer to company procedures to ensure compliance with company policy, law, and regulation. The root cause analysis drives whether the organization must enhance entity-level controls, transaction-level controls, or both.

Entity-level internal control enhancements typically include training, drafting policies and procedures, restructuring the compliance and internal audit functions, and periodic monitoring. Entity-level enhancements alone rarely suffice for companies facing SEC and FINRA sanctions. Mitigation of significant misconduct risk, as a practical matter, requires more than a strong control environment. Ironically, highly ethical companies often face greater risk because of the tendency to forget that not everybody (e.g., employees, customers, agents, suppliers, and investors) shares their commitment to integrity.

Transaction-level internal controls can be preventive or detective. Data-savvy companies save costs and increase effectiveness by developing forensic analytics to stop or uncover misconduct. When designing and assessing transaction-level internal controls, companies must pay special attention to the potential of collusion, management override, unauthorized access, and other forms of controls circumvention. An entity must be particularly careful of controls intended to address accidental errors and ensure that they adequately protect against intentional misconduct.

Discipline

The organization must take consistent and appropriate action. Discipline of primary actors is a given, although beware of business leaders trying to protect otherwise high-producing personnel.

Secondary actors pose the greater challenge. These include business leaders for exerting undue pressure and poor supervision as well as bystanders failing to report observed misconduct. Employees involved in financial reporting pose special challenges, as external auditors will be reluctant to place reliance or accept representations from individuals suspected of having engaged in misconduct.

Restitution

Both the Resource Guide and FINRA Reg. Notice 08-70 stress the importance of voluntary restitution. In 2012, FINRA reports doubled the remediation collected in 2011. Restitution raises delicate relationship issues, particularly when the alleged misconduct is not public. How, for example, does an organization inform a valuable client or customer that he or she was improperly overcharged without jeopardizing the relationship or causing additional unintended legal issues? How does the third party gain comfort that it is being made whole? Engaging a neutral third party can help satisfy victims and convince regulators of its veracity in regard to investigation and provide clarity on its ability to pay fees and penalties. A third party can also assist to quantify actual gains and losses, as well as the likely penalties.

Self-Reporting

Whether to self-report corporate misconduct is a complicated business and legal issue that requires investigating the facts, assessing various risks and benefits, and consulting extensively with counsel. FINRA Rule 4530 requires self-reporting of misconduct by an associated person or the member firm itself. While remediation is always an important step, it is essential if the company elects not to self-report. Consider, for example, Wal-Mart's alleged failure to remediate in its decision not to report corruption. A comprehensive and well-documented corrective plan assists to deflect government and public criticism if the misconduct is later discovered.

Independent Assessment of Remedial Measures

Independent assessment is essential if the organization seeks full remediation credit from the SEC or FINRA. The evaluator must be independent from the remediation team. Evaluate the program from a prosecutor's or regulator's perspective, that is, adequacy of the root control analysis, procedures to obtain assurance regarding misconduct, enhancement of entity and transaction controls, discipline, and restitution as described above. Next, evaluate the design and operating effectiveness of the remedial measures. We recommend including experienced auditors on the review team because the procedures to be used for conducting the evaluation are very similar to those used by auditors in auditing controls under Sarbanes-Oxley.

Conclusion

Timely and effective remediation makes good legal, business, and career sense. Fully implemented corrective measures to prevent recurrence demonstrate that the company takes responsibility for misconduct and should result in being rewarded with leniency from prosecutors, regulators, and other government officials. Remediation protects the company from future business loss, severe penalties and, at a personal level, professional reputation and career damage from recurrence of misconduct.

Related Practice Areas:

Forensic Accounting

Forensic Data Analytics

Fraud, Waste and Corruption Consulting

Remediation and Monitoring

Additional Links:

FCPA Resource Guide Highlights Need for Risks and Controls Experts

How Remediation Can Help Avoid Prosecution

Five Questions the Board Should be Asking

To Disclose or Not to Disclose: That is NOT the Only Question

STONETURN GROUP