Bloomberg BNA

Prevention of Corporate Liability
Current Report™

Remediation Can Help Firms Avoid Prosecution, Reduce Fines

BY JONNY FRANK

If remediation is done well, the organization possibly escapes prosecution, reduces monetary penalties, and avoids imposition of a monitor and other sanctions. Remediation done poorly—or worse, not at all—means the organization confronts prosecution, enhanced fines and penalties, difficult audit processes, and recurring financial loss.

Government and professional standard setters offer little specific guidance. Following are key steps and elements parsed from the Department of Justice,[1] the Securities and Exchange Commission,[2] U.S. Sentencing Commission[3] guidelines as well as frameworks and standards issued by the Committee of Sponsoring Organizations of the Treadway Commission, the Institute for Internal Auditors, the American Institute of CPAs, and other standard setters.

Bottom Line Affected

It is not just the organization that is impacted. Board members and senior management suffer embarrassment, as do business leaders, ethics and compliance officers, and internal auditors who must report that the organization has once again been victimized or engaged in misconduct. Worse, senior officers might even face criminal or civil prosecution under the ''responsible corporate officers'' doctrine, described sometimes as the ''crime of doing nothing.''[4]

The bright side is that remediation is good for business. Organizations lose somewhere between 2 percent and 5 percent of earnings to fraud and corruption, and these estimates do not include waste, abuse, fines, investigative and legal fees, insurance premiums, or lost opportunities.[5] Effective antifraud programs cut losses in half, saving most organizations millions of dollars in future losses.[6]

Government expectations are clear: Start remediation efforts early.

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 acted upon, albeit preliminarily, as the investigation progresses.

DOJ and SEC guidelines specifically consider whether an organization remediates promptly in deter-

[1] DOJ, Principles of Federal Prosecution of Business Organizations, U.S. Attorney's Manual, p. 9-28 (2008).

[2] SEC, Division of Enforcement, Enforcement Manual (2012).

[3] U.S. Sentencing Commission, Sentencing Guidelines, Chapter 8 (2011).

[4] See, e.g., Michael Clark, The Responsible Corporate Officer Doctrine, *Journal of Health Care Compliance* (February 2012).

[5] See, e.g., The Economist Intelligence Unit, Annual Global Fraud Survey, (2011) (organizations on average lose 2.1 percent of earnings to fraud), available at http://www.managementthinking.eiu.com/; ACFE, Report to the Nations on Occupational Fraud and Abuse (2012) (organizations lose the equivalent of 5 percent of revenue) available at www.acfe.com.

[6] ACFE Report to Nation. p. 42-44.

Jonny Frank, a partner in the Stone Turn Group, New York, served for 14 years as a partner at PricewaterhouseCoopers, where he founded and led the Investigations and Fraud Risks & Controls Group.

 ISSN 1067-6104

mining whether to file charges.[7] DOJ policy even allows timely remediation to cure compliance program flaws that gave rise to the misconduct. Swift remediation is essential to avoid a monitor as a condition of nonprosecution or deferred prosecution agreements or probation. Even if prosecution cannot be avoided, timely remediation substantially reduces the sentencing guideline culpability score, potentially saving millions of dollars in fines and penalties.[8]

If the allegations warrant an independent third party investigation, they likely also merit independent third party remediation, particularly if the organization is engaged in dialogue with prosecutors and regulators. Remediate, if possible, under the attorney-client privilege, as the process may unearth other misconduct.

Include Remediation Experts

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 when the investigation team is too busy to focus on remediation. Although the teams will be operating separately, coordination is essential and is best achieved if the remediation team communicates processes and results to the lawyer heading the investigation team. This ensures that remediation efforts remain in tune with the investigation findings.

Forensic accountants are not remediation experts. Remediation experts are to forensic accountants and investigators what cardiologists are to heart surgeons. Like cardiologists,

(continued on page 82)

(continued from page 84)

remediation experts apply specialized training to promote recovery and prevent and detect future problems on a timely basis, whereas forensic accountants and investigators, like heart surgeons, address known, immediate problems.

Remediation experts work in the absence of a specific allegation or suspicion. Investigators, in contrast, prove or disprove allegations. A remediation expert is knowledgeable in COSO internal controls, COSO enterprise risk management, and other frameworks for identifying and managing risks and is experienced in conducting risk assessments, evaluating the control environment and transaction-level control activities, and conducting forensic audits. The federal sentencing guidelines acknowledge this difference in expertise and specifically recommend the retention of outside remediation experts.[9]

Select a remediation adviser experienced in working and coordinating with legal teams—internal investigations 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 challenges in developing transaction-level control activities, key risk factors and indicators, data analytics, and monitoring and auditing.

Leverage Your Insiders

An experienced remediation expert can leverage internal auditors and other in-house resources to save time and cost. Independence is a consideration, particularly when defense counsel must persuade the government that the organization has implemented a comprehensive remediation program. An external remediation expert might be needed to vouch for the program, even if, say, internal audit does much of the legwork.

Internal auditors may not audit their own work.[10] Therefore, they cannot participate in creating and implementing changes to controls and policies that might be subject to a subsequent internal audit.

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, and control gaps.

Complex or significant misconduct warrants more systematic analysis. COSO, the globally recognized leading risk management framework, provides an effective and government approved structure, which encompasses these elements:

- The Control Environment: This refers to the corporate culture, including commitment to integrity, ''tone at the top,'' codes of ethics and conduct, mechanisms to report misconduct, training, etc. Remediation considers whether and how the control environment may have contributed to the underlying misconduct.
- Risk Assessment: This is the cornerstone of an effective antifraud and ethics and compliance program.[11] It is also the most commonly flawed part of the process (which is ironic, as without proper assessment the plan will almost certainly be incomplete). Remediation examines how the organization identifies and evaluates fraud and corruption risks. The process should be systematic rather than done on a haphazard or informal basis, and it should consider schemes and scenarios common to the industry sectors and markets in which the organization operates. The assessment considers whether the organization identified the risk and, if so, linked and evaluated the organization's 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: This refers to preventive and detective transaction level controls and ''design'' and ''operating'' effectiveness. Remediation evaluates design effectiveness by considering whether the transaction-level controls provide adequate protection and guard against collusion, management override, unauthorized access and other forms of circumvention. Remediation assesses operating effectiveness by employing audit procedures to determine if the controls are functioning as designed.
- Information and Communication: This refers to the information systems existing within an organization and how these systems communicate with one another as well as with employees who utilize and interpret the systems. In addition, this refers to the effectiveness of dedicated procedures related to internal and external communications related to a

[7] U.S. Attorney's Manual, 9-28.900; SEC Enforcement Manual 6.1.2.

[8] U.S. Sentencing Commission, *Chapter Eight Fine Primer: Determining the Appropriate Fine Under the Organizational Guidelines 4* (2011).

[9] U.S. Sentencing Guidelines, Section 8B2.1, commentary 6.

[10] Institute for Internal Auditors, Standard 1130A.1 (2012).

[11] See Jonny Frank, *Fraud Risk Assessment*, Internal Auditor (April 2004).

  BACM ISSN 1067-6104

variety of matters. Remediation assesses the effectiveness of the information systems and communications including the quality of the organization's antifraud and corruption knowledge management program.

■ Monitoring and Auditing: This includes contemporaneous and after-the-fact reviews to detect key fraud ''risk factors'' and ''risk indicators.'' Fraud risk factors are circumstances that impact likelihood of a fraud occurring, e.g., poor sales heighten risk of premature revenue recognition. Fraud risk indicators are red flags that the misconduct has or is occurring, e.g., an unusual spike in returns indicates a red flag of premature revenue recognition. Remediation considers effectiveness of procedures to identify risk factors and indicators, including the use of data analytics (anomaly testing) and enhanced technology.

Organizations must vigorously ferret out other misconduct throughout its remediation effort or they stand to lose creditability.[12] Imagine the embarrassment if the organization subsequently discovers that the perpetrators engaged in other wrongdoing or if comes out that the misconduct was pervasive.

In the absence of a specific allegation or suspicion, the remediation team can borrow the auditing principle of ''negative assurance''; that is, to gain comfort by conducting audit procedures to search for risk indicators or red flags.

When evaluating perpetrator misconduct, do not be fooled by tears, apologies, or expressions of regret—perpetrators rarely come completely clean. Use COSO risk assessment procedures to identify other ways that the perpetrators may have engaged in misconduct. Develop key risk indicators, and conduct forensic audit procedures, including data analytics, transaction testing and interviews, to gain negative assurance.

When evaluating misconduct by others, use the root cause analysis to frame procedures and gain assurance that similar misconduct has not occurred elsewhere in the organization. If the misconduct arose from poor operating effectiveness, the remediation team need only test whether control activities are operating effectively in a sample of other locations. However, if the problem was one of design effectiveness, the team may need to conduct substantive forensic audit procedures to search and identify key risk indicators.

DOJ, the SEC, and the sentencing guidelines instruct that organizations must modify transaction-level controls to prevent recurrence, which brings to mind the Chinese proverb, ''Easier said than done.''

Preventive controls often face substantial resistance because they add cost and inefficiency. The remediation team, if possible, should try to demonstrate a business case to gain acceptance at all levels in the organization.

Enhancing detective controls typically is the more practical long-term solution, although it requires more expense to develop than preventive controls. The process begins with identifying and re-engineering the schemes to pinpoint key risk factors and red flags. A team of remediation experts, information technologists, and business and finance personnel then develop data analytics and other early warning detection systems, operating innocuously in the background. The final steps are to develop a response protocol and to refine the process to reduce wasteful false positives.

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. The sentencing guidelines require discipline for failing to take reasonable steps to prevent or detect misconduct. This arguably includes discipline for exerting undue pressure, poor supervision, and failing to report observed misconduct.

'Delicate' Issues May Arise

Employees involved in financial reporting pose special challenges, as external auditors will not place reliance or accept representations from individuals suspected of having engaged in misconduct. Problems arise when, as is common, the investigation is inconclusive. The organization may find itself having to dismiss or transfer an employee if it is to get the auditor to sign off on the financial statements.

Both DOJ and the SEC stress restitution to victims as a significant factor in the charging decision. Making restitution payments raises delicate business issues, particularly when the alleged misconduct is not public information. For example, how does an organization inform a valuable client or customer that it was improperly overcharged without jeopardizing the relationship? How does the third party gain comfort that it is being made whole? Engaging a neutral third party can help to satisfy victims, convince the government of its veracity in regard to investigation, and provide clarity on its ability to pay fees and penalties.

How does an organization inform a valuable client or customer that it was improperly overcharged without jeopardizing the relationship?

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 with counsel.[13]

An organization that elects not to self-report faces an uphill battle to avoid prosecution and possibly a public relations nightmare if the conduct is later discovered.[14] However, being able to demonstrate that the organization conducted a comprehensive analysis of what went wrong and voluntarily and proactively implemented a program to prevent recurrence and reimburse victims goes a long way in deflecting criticism for not self-reporting.

Periodic auditing of the remediation program is essential for organizations seeking credit from the government for their remediation effort. The audit begins with an assessment of the development and design of the program; that is, the root control analysis, extended forensic audit pro-

[12] See sentencing guidelines, Section 8B2.1, commentary 2. (''Recurrence of similar misconduct creates doubt regarding whether the organization took reasonable steps to meet the requirements of this guideline.'')

[13] See Jonny Frank, To Disclose or Not To Disclose, Business Crimes Bulletin (July 2012).

[14] DOJ, the SEC, and the sentencing guidelines refer to self-reporting as a part of the remediation program. DOJ and the SEC guidelines include self-reporting as a factor to consider in deciding whether to file charges. The guidelines advise judges to reduce the culpability score by five points if the organization self-reports, fully cooperates in the investigation, and accepts responsibility for its conduct.

cedures, control activities enhancement, discipline, and restitution described above. The review also evaluates specific control modifications, considering both design effectiveness and validating operating effectiveness.

Remediation really is a choice between honey and vinegar. Business and legal rewards are ample, although the organization must commit to doing it well, invest time and resources, and accept risks. Doing a poor job, or none at all, produces short-term savings but exposes the organization to continued losses, bad press, and exacerbated legal penalties where the conduct exposes the organization to civil and criminal liability.

BACM ISSN 1067-6104