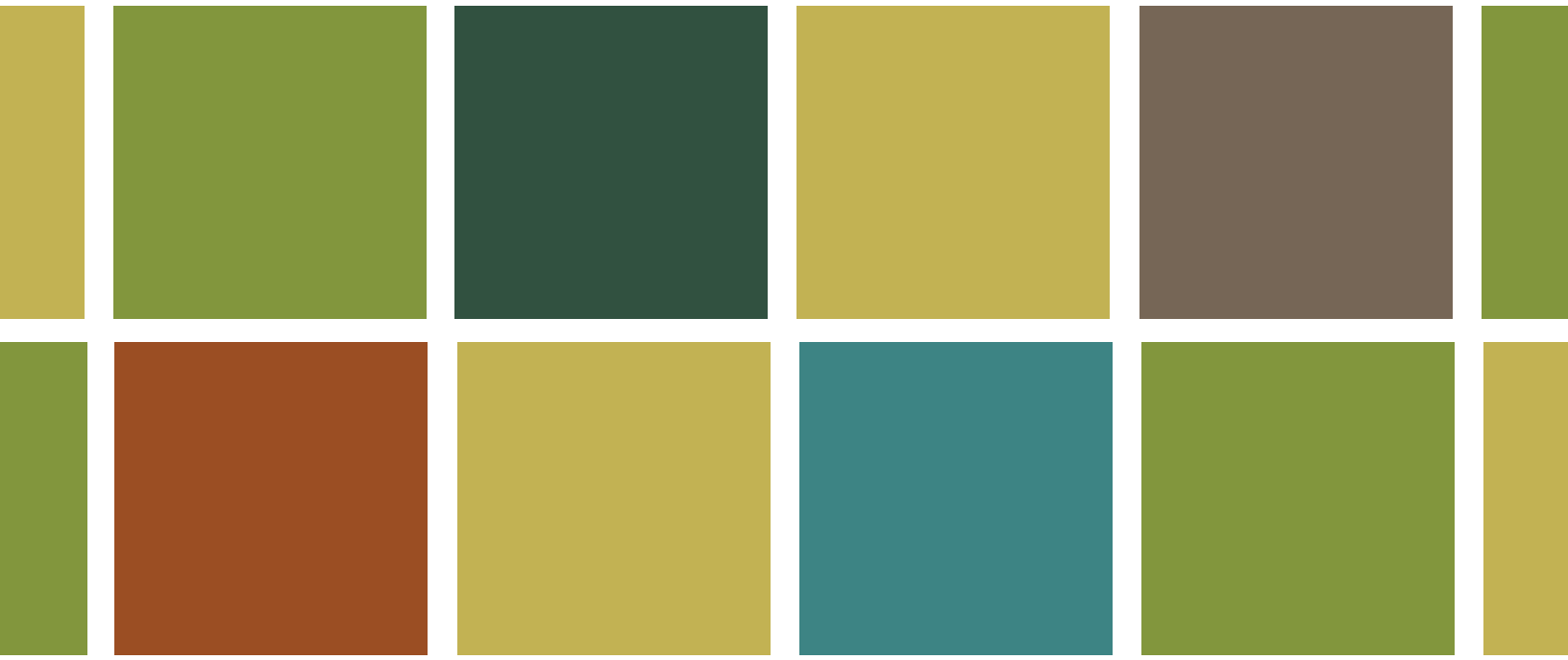
Remediation

LITIGATION SERVICES HANDBOOK: THE ROLE OF THE FINANCIAL EXPERT
5TH EDITION, CHAPTER 13A



STONETURN GROUP

StoneTurn Group

Jonny Frank

Remediation

LITIGATION SERVICES HANDBOOK: THE ROLE OF THE FINANCIAL EXPERT 5TH EDITION, CHAPTER 13A

Contents

13A.1 Introduction

Remediation is the corporate equivalent of medical rehabilitation. Just as patients recuperate and prevent recurrence, so too must organizations recover and prevent the recurrence of business misconduct. Remediation encompasses the following activities:

- Analyzing the root problems and causes
- Detecting other misconduct
- Disciplining the primary and secondary offenders
- Correcting compliance program and control weaknesses
- Considering self-reporting
- Making restitution to the victims
- Recovering damages from the offenders
- Restoring the corporate culture
- Repairing damaged internal and external relationships
- Independently assessing and auditing the effectiveness of the remediation and corrective measures

> “REMEDIATION IS THE CORPORATE EQUIVALENT OF MEDICAL REHABILITATION.”

(a) Legal Implications. Prosecutors, regulators, and professional standard setters all emphasize the importance of timely and effective remediation. The U.S. Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) regard remediation as a high premium.[1] Remediation helps organizations to avoid criminal prosecution and enforcement proceedings, to pay reduced penalties, and to escape a government-imposed compliance monitor.[2]

Remediation is a key component of an effective ethics and compliance program. The DOJ and SEC regard the guidelines of the United States Sentencing Commission (USSC) as the benchmark of an effective ethics and compliance program. To qualify as having an effective program under the sentencing guidelines,organizations must “take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization’s compliance and ethics program.”[3]

Other federal, state, local, and nonprofit agencies follow suit. The World Bank mitigates penalties by 50 percent or more for implementation of remediation and corrective measures to an organization’s compliance program.[4] The Financial Industry Regulatory Authority (FINRA), a nonprofit organization charged by Congress with protecting American investors, rewards remediation to “encourage firms to take immediate, proactive steps to correct systems, procedures and controls that may have contributed to problems that occurred at the firm.”[5] Banking and healthcare regulators have promulgated similar rules. At a local level, the New York District Attorney’s Office instructs prosecutors to consider remediation efforts when deciding whether to file criminal charges against an organization.[6]

Notwithstanding the government’s emphasis on remediation, prosecutors and regulators offer scant guidance on its specific elements. Nor do government authorities explain the criteria they consider and the processes they take to assess the effectiveness of an organization’s remediation efforts and corrective measures.

(b) Business Benefits. Remediation potentially provides more than just legal benefits. Although the principal objective is to recover from past misconduct, remediation also enhances the organization’s present and future antifraud program.

The professional literature includes numerous studies on the substantial direct and indirect costs of misconduct: fines, penalties, investigative and legal fees, higher insurance premiums, management distraction, lost productivity, talent flight, injured customer and supplier relationships, opportunity loss, and the erosion of brand value.[7] Effective remediation helps organizations to cut these losses by identifying and mitigating future misconduct risks.

13A.2 Remediation Versus Investigation

An investigation begins with a specific allegation or suspicion. The investigative team, typically led by a former prosecutor, conducts procedures to prove or disprove the alleged misconduct. The investigative team focuses on the *who*, *what*, *when*, and *where*.

Remediation professionals assist an organization in preventing future misconduct. Preventing recurrence requires that the organization focus on the *why* and *how*, and develop processes and controls to prevent and detect misconduct in the absence of an allegation or even a suspicion.

Investigative expertise does not always translate into expertise in remediation, just as firefighting does not always make the firefighters experts in fire safety. Attorneys are skilled at interviewing and fact-finding, but law schools do not train lawyers to perform risk assessments or to develop preventive and detective controls. Remediation professionals typically have an auditing and accounting background supplemented with experience in investigations and compliance monitoring. The sentencing guidelines specifically recognize this distinction and suggest that organizations retain advisers trained in remediation.[8]

(a) Requisite Knowledge, Skills, and Experience. Remediation requires a multidisciplinary team and the specific requisite competencies vary by engagement but often include the following:

- Risk management
- Operational and compliance controls
- Forensic audit
- Compliance and forensic analytics
- Governance, risk, and compliance
- Company-specific or industry knowledge

The remediation team should include individuals who are experienced in working and coordinating with legal, compliance, and finance teams. Although the remediation team should benefit from the findings of the investigation team, thorough and timely remediation processes often require a separate, concurrently retained, focused team. The remediation experts should understand misconduct risks and possess the skills to do the following:

- Identify the root causes of the misconduct
- Conduct fraud and compliance risk assessments
- Evaluate the design and operating effectiveness of the compliance controls
- Perform forensic audits

(b) Same or Different Firm or Team. Some organizations engage the same firm and team to conduct both the investigation and the remediation; others prefer separate firms or a single firm with separate teams. A single team could prove more efficient as long as the team is qualified to both investigate and remediate. A single team, however, invariably delays commencement of the remediation because investigators prefer to complete their investigation before turning to remediation. By that time, the organization has often lost interest in implementing an effective remediation program. Moreover, courts and agencies may treat remediation delayers less favorably than those who remediate promptly.

Whether it is the board or management that commissions the investigation, remediation is another consideration in the decision to hire the same firm

or different firms. Separate firms are needed when, as often occurs, the board (through counsel) investigates and management remediates.

13A.3 Independence And Privilege

Organizations often want to include their internal or external auditors. Professional standards prohibit auditors from auditing their own work, which effectively bars an internal auditor from an implementation role on the remediation team. [9]

A company must proceed carefully if it seeks to rely on remediation efforts to negotiate a more favorable government settlement. In such a case, the company should retain an independent third-party remediation expert to assess the remediation efforts and corrective measures and report them to the government. A third-party assessment carries more weight than an employee's counsel or outside counsel's.

Maintaining attorney-client privilege is essential if the remediation plan is likely to uncover wrongdoing beyond the scope of the original investigation. Consider forming two attorney-led work streams: one for investigation and another for remediation. Separate teams enable counsel to waive privilege to report on remediation while protecting privilege for the investigation. Separate teams also ensure the proper allocation of skill sets and avoid the remediation delays that invariably occur when the priorities of the investigation team do not allow it to focus on remediation. Although the teams will operate separately, they need to coordinate their efforts; to this end, the remediation team should communicate the processes and results to the leader of the investigation team to ensure that the remediation efforts remain in tune with and properly responsive to the investigation findings.

13A.4 When To Start

The government expects a firm to begin remediation immediately. Beyond asserting that it *will* take steps to prevent recurrence, a firm must prove that it has identified, considered, and taken preliminary action as the investigation progresses.

The government considers the promptness of an organization's remediation efforts in determining whether to file charges[10] or to impose a monitor.[11] Some prosecutors and regulators allow timely remediation to cure compliance program flaws that gave rise to the misconduct. Even if it cannot avoid prosecution or a monitor, timely remediation often reduces fines and penalties.[12]

Delay also jeopardizes the possibility that the organization will ever engage in meaningful remediation. Interest peaks at the start of an investigation. Internal investigations often prove distracting and expensive; they exhaust the firm and its employees physically, emotionally, and financially. At some point interest fades, and senior management and the board, having addressed the immediate crisis, invariably press for "closure." Management and the board tend to lose the appetite to remediate, notwithstanding significant legal, business, and reputation risks if misconduct were to reoccur.

13A.5 Root Problems And Causes

Root-cause analysis forms the foundation of effective remediation. Whereas investigation proves or disproves misconduct, root-cause analysis explores the root problems and underlying causes of the wrongdoing and its occurrence. The analysis frames the organization's efforts to ferret out other misconduct, assess appropriate discipline, enhance policies and controls, and conduct targeted followup monitoring and auditing.

Root-cause analysis answers the following questions:

- How did the offenders engage in misconduct?
- Why did they do it?
- How did they rationalize their misconduct?
- Why did preincident programs and controls fail to prevent and detect the misconduct?
- How can the organization prevent and detect future incidents?
- Where else should the team look for misconduct?

(a) Cressey's Fraud Triangle. According to Cressey's Fraud Triangle, named after the 1950s criminologist Donald Cressey, three conditions exist whenever misconduct occurs:

- Pressure or incentive
- Rationalization
- Opportunity[13]

(b) Pressures and Incentives. Pressures and incentives examine the mindset and motive(s) of the perpetrators. Comprehensive remediation analysis of the root causes considers all the major factors that contributed to the original misconduct. For example, one must avoid the temptation of blaming greed alone. Misconduct just as often results from the offender's attempt to avoid financial or personal loss: saving a job, escaping embarrassment, protecting family time, caring for a sick relative, and so on. The remediation team must consider the organization's role in creating unintended pressures and incentives. For example, a professional services firm that sets minimum billable time requirements incentivizes false time entries from employees who are concerned about job security. An organization that overloads duties and responsibilities pressures its employees to cut corners to get home.

(c) Rationalization. Cressey explains that offenders rationalize their misconduct—even billion-dollar fraudster Bernie Madoff reported how he justified his behavior to himself. Some common rationalizations that offenders cite are job dissatisfaction, denial of consequences, revenge for an actual or perceived prior harm or slight, family and health priorities, and "everybody does it."

Organizations tend to ignore this point of the fraud triangle and, as a result, forfeit an inexpensive opportunity to mitigate misconduct risk. If Cressey is correct that offenders need to rationalize their misconduct, it follows that organizations can reduce, if not eliminate, misconduct risk by eliminating the offender's ability to rationalize.

Conversely, the organization must understand the consequences of fostering an environment that allows offenders to rationalize misconduct. For example, if the organization engages in misconduct that benefits the company, it sets the tone for employees to engage in misconduct that benefits themselves.

(d) Opportunity: Controls and Compliance Program Flaws. Opportunity, the third point of Cressey's fraud triangle, means that the company should assess the effectiveness of its preincident compliance program and controls. Prosecutors and regulators also consider compliance program effectiveness when deciding whether to file charges, which charges to assert, and what penalties to impose.

Federal prosecutors, for example, must consider "the existence and effectiveness of the corporation's pre-existing compliance program" in determining whether to file criminal charges.[14] Similarly, the SEC considers "self-policing prior to the discovery of the misconduct, including establishing effective compliance procedures and an appropriate tone at the top."[15]

Serious misconduct exposes flaws in the preincident compliance program and controls. Compliance program flaws typically include a combination of the following factors:

- Failure to identify the risk
- Overreliance on controls
- Inability to identify and connect red flags

Assessment of the preincident compliance program and controls draws from the USSC guidelines, the Integrated Internal Controls Framework of the Committee of Sponsoring Organizations (COSO) of

the Treadway Commission, DOJ and SEC policy statements and pleas, and deferred-prosecution and nonprosecution agreements.[16] The remediation team should consider the control environment, risk assessment, control activities, information and communication, and monitoring and auditing.

(i) Control Environment. The control environment includes corporate culture, commitment to integrity, management's attitude, codes of ethics and conduct, mechanisms to report misconduct, and training.

Investigators should consider the following issues:

- Did the organization promote a culture that encourages ethics and compliance with the law, contractual agreements, and internal company policies?
- Did the organization demonstrate a commitment to a culture of compliance?
- Did the organization assign effective oversight and day-to-day responsibility for the ethics and compliance program?
- Did the organization provide adequate resources and direct board access to ethics and compliance personnel?

(ii) Risk Assessment. Ineffective risk assessment often leads to serious wrongdoing, for how can an organization expect to prevent a risk it has not identified? Remediation must consider the organization's risk assessment process and whether the organization anticipated the risk. Remediation must also consider whether the organization evaluated the effectiveness of its risk response. The remediation plan should correct weaknesses or deficiencies in the risk assessment process to ensure that the organization properly anticipates and addresses future risks.

The investigator should consider the following issues:

- Did the compliance program include risk assessment?
- Did the organization periodically assess and document the risk of the violation of laws, regulations, contractual obligations, company policies and processes, or other misconduct?
- Did management participate in the risk assessment?
- Did the risk assessment anticipate the wrongdoing? If it did not, why not? If it did, has the organization identified and evaluated its risk response?

(iii) Control Activities. An organization develops control activities to ensure compliance with the law, regulations, contractual obligations, and company policies and processes. Controls can be at the entity or transaction level, preventive or detective, and automated or manual. For example, to mitigate procurement fraud, companies use approved vendor lists and segregate duties to require that separate employees request, approve receipt, and issue the payment to the vendor.

The investigator should consider the following issues:

- Did the organization promulgate visible and clear policies, processes, and controls?
- Were the controls effectively designed (i.e., assuming that they operated effectively, did they provide adequate protection from collusion and circumvention)?
- Were the controls operating effectively (i.e., were they operating as designed)?
- Did the personnel who performed the control possess the necessary authority and competence to do so effectively?
- Did a clear and rational link exist between the risk assessment and the control activities?

(iv) Information and Communication. Information and communication systems exist within an organization and interact with one another as well as with the employees who use and interpret the systems. This element also refers to the effectiveness of the procedures dedicated to internal and external communications.

Investigators should consider the following issues:

- Did the organization have and publicize a system (including mechanisms allowing for anonymity and confidentiality) whereby employees and agents could report or seek guidance on ethics and compliance issues without fear of retaliation?
- Did the organization communicate its policies effectively to the directors, employees, joint venture partners, agents, suppliers, and other relevant third parties?
- Did the organization provide adequate training, including annual certification, and a resource to provide advice?
- Did the organization make adequate use of technology, including compliance systems, forensic analytics (the use of data to investigate alleged or suspected misconduct), compliance analytics (the use of data to prevent and detect compliance and control violations), and security systems?

(v) Monitoring and Auditing. Monitoring refers to contemporaneous company reviews to (1) evaluate the design and operating effectiveness of controls, and (2) detect misconduct. *Auditing* refers to similar reviews conducted on an after-the-fact basis.

Investigators should consider the following issues:

- Did the organization conduct monitoring and auditing procedures on the wrongdoing at issue?
- If it did not, why not?
- If it did, did the monitoring and auditing procedures include specific risk indicators?
- Would effective monitoring or auditing have more rapidly detected the misconduct?

13A.6 Remote or Pervasive

Imagine the legal implications—and embarrassment—if the government discovers that an organization's internal investigation failed to detect the full extent of the wrongdoing or similar schemes committed by others in the organization. Organizations cannot afford to assume that any incident is an isolated event. The wrongdoing is often much more extensive than originally believed.

Building on the root-cause analysis, remediation professionals can assess the likelihood of undetected misconduct by the wrongdoers or others in the organization. The remediation team should document its conclusion and rationale, especially if it decides that the wrongdoing is an isolated event and warrants no further action from the organization. Contemporaneous documentation will be useful if later events reveal an incorrect assessment by the company.

How does an organization ferret out undetected misconduct in the absence of specific allegations or suspicions to guide the investigators? Even worse, how does the organization prove the absence of misconduct?

Remediation professionals borrow from an auditing process called *negative assurance*. In this process, the remediation team searches for indicators of misconduct. If the team finds none, it provides negative assurance to management and the board that it has not detected anything to indicate the occurrence of misconduct. For example, suppose that the wrongful conduct involved premature revenue recognition and that the remediation team identified returns after a quarter's end as a risk indicator. An absence of a spike of returns would provide negative assurance that the organization did not engage in premature revenue recognition.

(a) Wrongdoer Misconduct. Experienced investigators know that wrongdoers often engage in a variety of misconduct and rarely come completely clean even when they have made a confession. Remediation experts apply the following five-step forensic auditing process to assess whether the organization has captured the full extent of the wrongdoing:

1. Identify potential misconduct risks by examining the wrongdoers' pressures, incentives, and opportunities to engage in misconduct.
2. Examine the design and operating effectiveness

of the organization's risk response.

3. Create risk indicators and red flags for residual risks.
4. Develop forensic auditing procedures, including forensic analytics, transaction testing, accounts and balances testing, walk-throughs, observations, and interviewing.
5. Provide negative assurance if forensic auditing procedures do not identify risk indicators; refer for investigation when sufficient indicators and red flags exist.

Consider the following example: The company conducts a risk assessment after terminating Salesman A for travel and expense abuse. The assessment identifies that Salesman A has had an incentive and the opportunity to inflate sales numbers (and his bonus) through side agreements that give customers the right of return. These side agreements caused improper revenue recognition and could have resulted in a financial misstatement.

A disproportionate spike in sales just before the end of a quarter or in returns just after the end of a quarter would be a classic risk indicator. The absence of a spike in sales or returns would lead the remediation team to provide negative assurance that there are no indications of premature revenue recognition. The presence of a spike would give rise to a suspicion, which the remediation team would refer to the organization for investigation.

(b) Misconduct by Others. Remediation professionals need to consider whether to search for similar misconduct elsewhere in the organization. For example, suppose that a multinational company discovers corruption in a sales office in Africa. How does it investigate whether similar wrongdoing occurred in other high-risk jurisdictions?

Investigating the existence of misconduct throughout an organization will prove expensive and time-consuming. In the absence of a specific allegation or suspicion, the inquiry resembles a forensic audit rather than an investigation.

Such inquiries can be mandatory or voluntary. Prosecutors, regulators, external auditors, investors, and other external stakeholders sometimes demand that the organization look for other misconduct. For voluntary investigations, the organization needs to balance the time and expense of conducting extended forensic auditing procedures with the business, legal, and reputational consequences of permitting wrongdoing to go undetected.

The remediation team begins with the flaws in the compliance program and controls that have been identified in the root-cause analysis. Assume, for example, that the controls are well designed but are not operating effectively; that is, the controls would adequately militate against wrongdoing if they were operating as designed. Under these circumstances, the remediation team would test operating effectiveness in a sample of other locations. Audits that demonstrate success of the controls elsewhere in the organization would support the conclusion that the wrongdoing was limited to a single individual or location.

Forensic auditing becomes more difficult if root-cause analysis reveals deficiencies in design effectiveness; that is, the control, even if operating effectively, would not adequately militate against the risk of misconduct. Under those circumstances, the remediation team must undertake substantive procedures to determine whether others in the organization exploited the design flaws. The forensic auditing procedures would be similar to those used in assessing whether the investigation fully captured the extent of the wrongdoers' misconduct. These procedures are as follows:

- Identify the risks.
- Create risk indicators and red flags.
- Develop forensic auditing procedures, which include forensic analytics, transaction testing,

accounts and balances testing, walk-throughs, observations, and interviewing.

- Provide negative assurance if the forensic auditing procedures do not identify any risk indicators, or refer for investigation if the auditing procedures identify sufficient indicators and red flags.

13A.7 Discipline of Primary and Secondary Actors

Effective remediation requires consistent and appropriate discipline. The sentencing guidelines criteria, for example, require that organizations consistently impose "appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct." The DOJ and SEC similarly require that disciplinary measures be "fairly and consistently applied across the organization."[17] Discipline includes termination, suspension without pay, financial penalties, and demotion. Business leaders will sometimes try to protect otherwise productive personnel. DOJ and SEC policies warn that no person within an organization is too valuable to face discipline.[18] If the employee performs an important function, the organization must prepare contingency plans to deal with the possible departure. Such preparation includes identifying a temporary or permanent replacement (should the need arise) to ensure minimal business interruption from remediation. The organization needs to apply disciplinary measures consistently across pay grades, treating high-ranking employees at company headquarters similarly to lower-ranking ones in the field.

Secondary actors pose a greater challenge and fall into two categories: **(1)** business leaders who supervise negligently or exert pressure, and **(2)** bystanders who fail to report observed misconduct. Employees involved in financial reporting present an extra challenge, since external auditors will be reluctant to rely on or accept representations from individuals suspected of having engaged in misconduct.

13A.8 Enhancing Compliance Program and Controls

Root-cause analysis will identify deficiencies in compliance program and controls.

The remediation team should also look for guidance in past government plea and settlement agreements. In Foreign Corrupt Practices Act (FCPA) matters, for example, the DOJ and SEC often specify mandatory enhancements to organizations' anticorruption compliance programs and controls.[19]Practitioners find it faster and easier to identify control deficiencies than to correct them. The effort requires active involvement and careful coordination among the remediation team, business functions and units, and legal and compliance groups. Change in one process often affects others. For example, changes in a company's accounting requirements for recognizing a sale might affect sales personnel incentive pay structures. The organization should document its corrective action plan, including specific milestones and timetables.

The remediation team must also take steps to encourage affected employees, vendors, agents, and customers to embrace the required policy, process, and control changes. Such efforts include the following:

- Publicizing the benefits to the individual and organization
- Obtaining the support of senior management
- Instituting regular updates to verify ongoing compliance, including a constant process improvement expectation

Blaming the government (e.g., "we are making these changes because the government requires it") leads to non-compliance. If the team anticipates resistance from the organization, it will need to

develop additional controls to ensure compliance.

Detective controls (e.g., monthly reconciliations) often prove less expensive and disruptive than preventive controls (e.g., hiring additional personnel to create a segregation of duties). Employees perceive the latter measures as creating unnecessary impediments. Firms also find automated controls and compliance analytics (e.g., system-generated comparisons to ensure that the vendor appears on the master vendor list) more acceptable, though expensive, to implement.

13A.9 Self-Reporting

Prosecutors and regulators emphasize the importance of an organization's self-reporting misconduct to the government. When deciding whether to pursue criminal charges, federal prosecutors "consider whether the company made a voluntary and timely disclosure as well as the company's willingness to provide relevant information and evidence and identify relevant actors inside and outside the company, including senior executives."[20] The sentencing guidelines reward organizations that self-report to government officials "within a reasonably prompt time after becoming aware" of the misconduct.[21]

In pursuing civil charges, SEC enforcement attorneys consider whether the organization self-reported "misconduct when it is discovered, including conducting a thorough review of the nature, extent, origins, and consequences of the misconduct, and promptly, completely, and effectively disclosed the misconduct to the public, to regulatory agencies, and to self-regulatory organizations."[22]

Whether to self-report serious misconduct is a complicated matter that requires investigating the facts and assessing the legal, business, and reputational risks. Government agencies vary on the degree of benefit that a firm gains from self-reporting. At the federal level, benefits can vary geographically; for instance, a local branch office might have a track record of giving more or less credit than the agency's headquarters. When deciding whether to self-report, an entity should assess the quality of its remediation efforts and, if these are lacking, perform a comprehensive and defensible remediation process to identify issues or misconduct.

(a) Likelihood of Becoming Public. A decision against self-reporting carries a high risk in today's environment. As a practical matter, organizations should assume that the allegations will become public and prepare for that risk. Social media provides an easy outlet for disgruntled employees and others. Whistle-blowers—auditors, compliance officers, officers, directors, and other insiders—can receive hefty rewards by reporting misconduct.[23] In 2014, the DOJ authorized $435 million in rewards to False Claims Act relators.2[24] That year, the SEC approved an award of more than $30 million to a single whistle-blower.[25] In 2012, the IRS authorized a $104 million reward.[26] Other federal, state, and local government agencies have similar programs.

(b) Thoroughness of the Investigation. Many organizations, particularly those leaning against self-reporting, curtail investigations. This is a mistake. An organization cannot properly decide whether to self-report without knowing the facts. If the government becomes aware of the allegations, it will assess the investigation's independence, competency, scope, and quality. The legal sanctions and damage to the firm's reputation will worsen if the organization appears not to have pursued allegations of misconduct.

(c) Adequacy of the Remediation. Remediation is crucial if the organization decides against self-reporting. If the misconduct becomes public, the organization must demonstrate that it has taken all necessary action to prevent recurrence in order to mitigate legal risks and damage to its reputation.

(d) Legal, Regulatory, and Professional Obligations. Some regulations and professional affiliations carry an affirmative duty to report. For example, the Federal Acquisition Regulations require government contractors and subcontractors to report any credible evidence of a violation of federal criminal law involving fraud, conflict of interest, bribery, or gratuity.[27] Likewise, professional standards require auditors to take action if they discover evidence of a crime during an audit.[28] Members of such professions should check with counsel and document their conclusions.

(e) Likelihood of Sanctions if the Government Discovers Misconduct. Whether and to what extent the government will impose sanctions if it discovers the misconduct rests on several factors:

- Magnitude of the misconduct
- People involved
- Victims
- Length of time of the misconduct
- Amount of funds involved
- Why the controls failed to prevent or detect the misconduct
- Remedial steps that the organization has implemented

Prosecutors tend to establish internal, non-binding guidelines for the cases they will prosecute. These guidelines vary by jurisdiction, so counsel should have familiarity with the jurisdiction at issue. The government will assess the quality of the firm's investigation and the depth of the remediation. Even though counsel could present good arguments to defend the decision against self-reporting in some cases, the prosecutor could nevertheless decide to take a harsher stance to deter others from not self-reporting.

13A.10 Restitution and Recovery

Restitution to victims is essential to remediation, including whether the organization made restitution voluntarily or waited for a court order. Every prosecutor and regulator considers restitution in assessing an organization's remediation efforts.

Recovery is the flip side and refers to the organization's efforts to secure compensation when it is the victim of wrongdoing. Quantifying victim loss—whether it be for purposes of making restitution or seeking financial recovery—is not always straightforward. Complex matters require input on damage from valuation experts, similar to civil litigation procedures.

13A.11 Damaged Culture and Relationships

Separate from preventing recurrence, the organization needs to take action to restore damage to the corporate culture and to its internal and external relationships. This chapter does not address this subject in detail because accountants do not participate directly in this.[29]

Accountants should be sufficiently familiar with the topic to ensure that the organization takes appropriate steps. When allegations of misconduct arise, organizations focus almost exclusively on resolving urgent legal issues. Organizations commonly disregard the collateral impact on corporate culture and relationships— hugely significant business issues that are easily overlooked in the midst of a legal crisis.

Organizations need to address the inevitable distraction and ensuing loss of productivity, continue to motivate the current employees, and attract and retain top performers. The organization must also protect and nurture third-party relations, whether with investors, joint venture partners, vendors, or customers. The remediation team, unless it is equipped with resources to do so, needs to counsel business leaders to ensure that the organization addresses these issues.

APPENDIX: Assessing the Remediation Program

This appendix lists issues for prosecutors, regulators, board members, counsel, compliance officers, auditors, and professional advisers to consider when assessing the quality and effectiveness of the remediation program. The assessment team cannot be the same team that developed and implemented the program.

Knowledge, Skills, Experience, and Independence

- Did the team include experts in prevention and detection of misconduct in the absence of an allegation or a suspicion?
- Did the team include experts in risk assessment, developing and auditing controls, compliance analytics, and auditing, along with company-specific and industry experts?
- Did the team include personnel involved directly or indirectly in the wrongdoing?
- Will any team members (e.g., internal auditors) be assessing their own work?

Timelines

- Did the organization begin remediation promptly after the discovery of misconduct?
- Has the organization already implemented corrective measures, or is it waiting until after the settlement?

Root Problems and Causes

- Did the organization identify any incentives and pressures that led to the misconduct?
- Did the organization consider how the wrongdoers rationalized their actions?
- Did the organization assess and identify weaknesses in the preincident compliance program and controls? These include weaknesses related to the following factors:
    - Control environment
    - Risk assessment process
    - Design and operating effectiveness of control activities
    - Information and communication, including forensic and compliance analytics
    - Adequacy of contemporaneous monitoring and after-the-fact audits

Remote or Pervasive

- Did the organization document its rationale if it concluded that the wrongdoing was an isolated event?
- Did the organization conduct adequate procedures to detect the full extent of the wrongdoing?
- Did the organization identify other opportunities to engage in misconduct, evaluate the design and operating effectiveness of the risk response, and conduct forensic auditing procedures to detect risk indicators and red flags?
- Did the organization conduct adequate procedures to detect whether others engaged in similar wrongdoing? These would include testing of the controls' effectiveness and conducting forensic auditing procedures to detect risk indicators and red flags.

Discipline of Primary and Secondary Actors

- Did the organization employ a fair and consistent disciplinary process, or did top producers or senior personnel receive special dispensations?
- Did the organization take appropriate disciplinary measures for the creation of inappropriate incentives and pressures, negligent supervision, and the failure to report observed misconduct?

Enhancing Compliance Programs and Controls

- Did the organization take appropriate measures to correct the compliance program and control deficiencies identified during the root-cause analysis?

- Did the organization implement the corrective measures required by prosecutors and regulators in similar matters?

Self-Reporting

- Did the organization consider, on the advice of counsel, whether to self-report misconduct to the authorities?
- Did the organization's assessment of whether to self-report consider the legal obligations to report, the likelihood and consequences of government discovery, the thoroughness of the investigation and remediation, legal incentives, and the financial and reputational implications?

Restitution and Recovery

- Did the organization take appropriate steps to quantify the loss and identify, notify, and make full restitution to the victims?
- Did the organization make restitution voluntarily, or did it wait for a court order?

Periodic Assessment and Audit

- Does an independent party periodically assess the remediation process and the implementation of corrective measures?
- Does the organization periodically audit the new and enhanced processes and controls?

Notes

[1] DOJ and SEC, A Resource Guide to the U.S. Foreign Corrupt Practices Act at 57–58 (Nov. 2012) ("Resource Guide"). See also DOJ, United States Attorney's Manual, 9-28.900; SEC, Enforcement Manual, §6.2.1. (2013).

[2] DOJ and SEC, A Resource Guide to the U.S. Foreign Corrupt Practices Act at 57–58 (Nov. 2012); DOJ, United States Attorney's Manual, 9-28.900; SEC, Enforcement Manual, §6.2.1. (2013).

[3] USSC, Guidelines Manual, §8B2.1 (b) (7) (2013).

[4] World Bank Office of Suspension and Debarment, Report on Functions, Data and Lessons Learned 2007–2013 (2014).

[5] FINRA, FINRA Provides Guidance regarding Credit for Extraordinary Cooperation, Regulatory Notice 08-70 (Nov. 2008).

[6] Daniel R. Alonso, Consideration in Charging Organizations, N.Y. Cnty. Dist. Attorney's Office (May 27, 2010), http://manhattanda.org/sites/default/files/Considerations%20in%20Charging%20Organizations.pdf.

[7] Dow Jones, Anti-Corruption Survey Results (2014); Association of Certified Fraud Examiners, Report to the Nations on Occupational Fraud and Abuse (2014); Economist Intelligence Unit, 2013–2014 Global Fraud Report (2013); James R. Gregory, Corporate Brand Value (2011).

[8] USSC, Guidelines Manual, §8B2.1, commentary 6 (2011).

[9] Institute of Internal Auditors, International Standards for the Professional Practice of Internal Auditing, §1130A.1 (2010).

[10] USAM 9-28.900; Enforcement Manual §6.2.1.

[11] FCPA Resource Guide at 71.

[12] See, e.g., USSC, Chapter Eight Fine Primer: Determining the Appropriate Fine under the Organizational Guidelines 4 (2011).

[13] Joseph T. Wells, Principles of Fraud Examination, 2nd ed. (Donald Fowley, ed., 2008).

[14] DOJ, U.S. Attorney's Manual, 9-28.900; SEC, Enforcement Manual, §6.2.1. (2013).

[15] SEC, Enforcement Manual, §6.2.1. (2013).

[16] For information about COSO, see http://www.coso.org.

[17] DOJ and SEC, Resource Guide, 57–58.

[18] Ibid.

[19] Jonny Frank, "Key Elements of FCPA Remediation," Business Crimes Bulletin, Mar. 2013.

[20] DOJ and SEC, Resource Guide, 54.

[21] USSC, Guidelines Manual, 8C2.5 (g).

[22] SEC Enforcement Manual, §6.2.1. (2013).

[23] Jonny Frank, Companies That Fear Whistleblowing under New SEC Rules Can Mitigate Risk, Use Attorney-Client Privilege Strategically, Prevention Corp. Liab. (BNA), Oct. 2011.

[24] U.S. Dep't of Justice, Justice Department Recovers Nearly $6 Billion from False Claims Act Cases in Fiscal Year 2014 (Nov. 20, 2014). http://www.justice.gov/opa/pr/justicedepartment-recovers-nearly-6-billion-false-claims-act-cases-fiscal-year-2014.

[25] SEC, 2014 Annual Report to Congress on the

Dodd-Frank Whistleblower Program (2012).

[26] David Kocieniewski, "Whistle-Blower Awarded $104 Million by I.R.S.," New York Times, Sept. 12, 2012.

[27] Federal Acquisition Regulations §52.203-13 (2008).

[28] Section 10A of the Securities Reform Act of 1934, 15 USC 78j-1), (b)(1); American Institute of Certified Public Accountants Auditing Standards Board, Statement of Auditing Standards, 54.

[29] Jonny Frank and Alan Hack, "Preserving Human Capital in Legal Crisis," Law 360 (Jul.16, 2012). http://www.law360.com/articles/359128/preserving-human-capital-in-alegal-crisis.

"Remediation," by Jonny Frank is an excerpt from Weil, Roman L., Litigation Services Handbook: The Role of the Financial Expert (5th ed.). Wiley, 2015.

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