Key Elements of Effective FCPA Remediation:  
*Earning DOJ and SEC’s “High Premium”*

Both the Department of Justice (“DOJ”) and Securities Exchange Commission (“SEC”) place a “high premium” on remediation efforts.1 Organizations that satisfy those expectations may avoid criminal prosecution and enforcement proceedings; obviate a government imposed compliance monitor or independent consultant2; pay reduced penalties and safeguard brand value.

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 suffer the same.

Better yet, effective Foreign Corrupt Practices Act (“FCPA”) remediation adds to the bottom line and should pay for itself many times over. According to independent studies, corporations, on average, lose 2% of earnings to fraud and corruption or the equivalent of a full week’s work.3 Roughly 20% of companies lose over 4% of earnings or the equivalent of two week’s work and a quarter of those lose over 10% of earnings.4

High corruption risk correlates to high fraud risk. Companies doing business in emerging markets face higher than average losses absent effective and proactive antifraud program and controls. Nearly 60% of companies delay or avoid global business opportunities due to concern over fraud and corruption.5

Government expectations are rigorous and, no surprise, the bar continues to rise. The most detailed guidance appears in the attachments to DOJ corporate deferred and non-prosecution agreements.6 Additional guidance appears in the DOJ Principles of Federal Prosecution of Business Organization, SEC Enforcement Manual and Chapter 8 of the US Sentencing Guidelines (“USSG”) and The FCPA Resource Guide. This article suggests a practical plan for organizations and counsels to meet these expectations.

**USSG: Involve Remediation Advisers**

The 2011 amendments to the USSG suggest that organizations include professional advisers in their remediation efforts.7 Remediation is different from forensic accounting. Remediation experts work in the absence of a specific allegation or suspicion and apply specialized knowledge, skills and training to promote recovery and prevent recurrence.

Select a remediation advisor experienced in working and coordinating with legal teams – while the remediation team should be benefiting from the findings of the investigation team, thorough and timely remediation processes often require a separate, concurrently retained, focused team. The remediation

---

* Jonny Frank, a partner in the New York office of the StoneTurn Group, served for 12 years a federal prosecutor and 14 years as a partner from PwC, where he founded and led the Investigations and Fraud Risks & Controls. He also served on the faculties of the Yale School of Management, Fordham University School of Law, and Brooklyn Law School, where he taught courses in Fraud & Corruption Management, International Criminal Law and Complex Investigations. Rex Homme, a partner in StoneTurn’s Chicago office, has over 20 years’ experience supporting law firms and companies to prevent, detect, and investigate fraud and corruption worldwide.
experts should be knowledgeable of corruption risks and skills and be experienced in helping lawyers and organizations to identify root causes of misconduct, conduct anticorruption risk assessments, evaluate entity and transaction levels controls and perform forensic audits.

Consider also whether the remediation adviser should come from a different firm than the forensic accountants that assisted in the investigation. Does counsel represent management or the board? If retained by management’s counsel, the remediation expert works alongside and helps the remediation team conduct a root cause analysis and implement new policies, procedures and controls. When assisting counsel to the board, the remediation adviser assesses the design and operating effectiveness of remedial measures akin to that of an independent monitor.

**Independence and Privilege**

Independence is another consideration, particularly if the organization is seeking to avoid a government imposed compliance monitor or independent consultant. The remediation adviser cannot audit its own work.\(^8\) The government will not consider a remediation adviser to be independent if it develops or implements the remediation plan or serves as the client’s advocate.

Maintaining the attorney client privilege is essential if the remediation efforts might uncover other corporate misconduct. 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 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 to ensure that remediation efforts remain in tune with the investigation findings.

**Do Not Delay or Wait Until End of Investigation**

Government expectations are clear: commence remediation immediately. 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 actioned, albeit preliminarily, as the investigation progresses.

The DOJ and SEC specifically consider whether an organization remediates promptly in determining whether to file charges\(^9\) or impose a monitor.\(^10\) DOJ policy even allows timely remediation to cure compliance program flaws that gave rise to the misconduct. Even if it cannot avoid prosecution, timely remediation substantially reduces the USSG culpability score, potentially saving millions of dollars in fines and penalties.\(^11\)

Some attorneys and organizations delay remediation until the investigation is complete. This is a mistake. Delay allows for the risk of continued violations and thereby exposing the organization to harsher sanctions and likely imposition of a government compliance monitor or independent consultant. Delay creates a practical challenge apart from legal implications. Internal investigations are physically, emotionally and financially exhausting. Sooner or later, management presses for “closure.” The appetite for remediation is lost or invariably diminished.

**Root Cause Analysis**

The “Cressey Fraud Triangle,” named after 1950s criminologist Donald Cressey, provides a useful and simple framework for conducting a root cause analysis in simple matters.
According to Cressey, three conditions exist whenever misconduct occurs: 1) incentive or pressure, (2) opportunity, and (3) rationalization. The analysis thus considers motivation(s) and justification(s) for paying bribes, as well as control gaps that enabled unauthorized use of company assets.

Complex or significant misconduct warrants deeper analysis, most frequently, the COSO framework, which is globally recognized and expressly approved by the SEC. As further detailed below, the COSO framework entails an analysis of the control environment, risk assessment, control activities, information and communication, and monitoring:

- **Control Environment** refers to the corporate culture, including commitment to integrity, “tone at the top,” codes of ethics and conduct, mechanisms to report misconduct, training, etc. The root cause analysis should consider how the control environment may have contributed to bribe paying.

- **Risk Assessment** is “fundamental,” say the DOJ and SEC, an effective anticorruption ethics and compliance program. A corruption root cause analysis considers the organization’s risk assessment process, whether it anticipated the bribe 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** refer to preventive and detective transaction-level controls and “design” and “operating” effectiveness. Most bribery schemes involve flawed internal controls. The root cause analysis should determine whether the flaw was a matter of design effectiveness, operating effectiveness or both.

- **Information and Communication** 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. This element also refers to the effectiveness of dedicated procedures related to internal and external communications related to a variety of matters. The root cause analysis should assess the effectiveness of the information systems and communications, including the quality of the organization’s antifraud and corruption knowledge management program.
• Monitoring and Auditing includes contemporaneous and after-the-fact reviews to detect misconduct “risk factors” and “risk indicators” and to identify whether the controls are effective in addressing them. Risk factors are circumstances that impact likelihood of misconduct occurring, e.g., a high score from Transparency International heightens risk of corruption. Risk indicators are “red flags” that the bribery has or is occurring, e.g., offshore payments to a third party. The root cause analysis should consider the quality of the company’s monitoring and auditing systems and whether the misconduct was timely detected.

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

• 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 audit procedures, including data analytics, transaction testing and interviews, to gain negative assurance.

• Misconduct by Others – Use the root cause analysis to frame procedures to gain assurance that similar misconduct has not occurred elsewhere in the organization. If the misconduct arose from poor operating effectiveness, test whether control activities are operating effectively in a sample of other locations. If, however, the problem was one of design effectiveness, the team might need to conduct substantive forensic audit procedures to search for red flags of similar misconduct.

Corruption Risk & Controls Register
The DOJ and SEC specifically evaluate an organization’s corruption risk assessment process when assessing a company’s compliance program and FCPA deferred prosecution agreements usually include a requirement that the company identify and assess risks of potential foreign bribery. Corruption risk assessments generally involve (a) identifying interactions between the organization and public officials and (b) potential methods to pay bribes. Begin by developing a framework that the company can use day-to-day. Suggested fields include (a) description of bribe scheme or scenario, (b) source for including scheme in inventory, (c) impacted business units or functions, (d) inherent likelihood and significance, (e) preventive and detective controls, (f) residual likelihood and significance, and (g) residual risk response including forensic data analytics.

Next develop an inventory of potential bribe schemes. Remediation advisers can jumpstart the process. Research schemes endemic to the industries and markets where the company does business. Perform interviews and hold focus groups among relevant business unit and function leaders. Consider past allegations at the company, as well as the results of internal audits and business reviews of foreign business units and functions.

The team then assesses the likelihood and significance of a scheme occurring on an “inherent” basis; that is, without regard to existing controls. The next step is to link and evaluate controls relied upon by the organization to mitigate risks assessed as likely or significant. If existing controls do not lower the risk to an acceptable level, the team must devise a residual risk response, typically combining preventive and detective controls and forensic data analytics.

Keep the register up-to-date. This critical, but often overlooked, step is simple and not time consuming, if the organization assigns responsibility for updating the register based on new whistleblower allegations, internal audits, business reviews, and media reports.
Control Environment and Entity-Level Controls
The DOJ and SEC, as well as USSG criteria of an effective ethics and compliance program require companies to take steps to enhance the control environment. Common DOJ and DPA agreements require that the organization:

- Promote an organizational culture that encourages ethical conduct and a culture of compliance;\(^{17}\)
- Use reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the Company knew, or should have known engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program;\(^{18}\)
- Develop “clearly articulated” FCPA policies;\(^{19}\)
- Assign a corporate executive with responsibility for the implementation and oversight of compliance standards and procedures, authority to report matters directly to the Board and appoint heads of compliance for each of its business units;\(^{20}\)
- Develop mechanisms to communicate policies, standards and procedures to all directors, officers, employees, agents and business partners, including, periodic training and annual certification; and
- Develop a system for (a) providing guidance and advice, (b) reporting information on a confidential basis, and (c) responding to reports of misconduct or requests for advice.\(^{21}\)

Transaction-Level Controls
Transaction level controls refer to procedures to ensure compliance and prevent and detect non-compliance with specific company policies. Organizations need to guard against weaknesses in both design and operating effectiveness. Design flaws involve inadequate protection against collusion, management override, unauthorized access and other forms of controls circumvention. Operating effectiveness refers to whether the controls are functioning as designed.

The remediation program must develop or enhance transaction-level controls to prevent recurrence of misconduct identified during the FCPA investigation as well as significant risks identified during the corruption risk assessment. Common DOJ and SEC mandated transaction-level controls enhancements require that the organization:

- Promulgate controls governing gifts, hospitality, customer travel, political contributions, charitable donations, facilitation payments, and solicitation and extortion;
- Modify internal controls so that they are reasonably designed to ensure accurate books and records, and accounts to ensure that they cannot be used for the purpose of foreign bribery or concealing misconduct;
- Institute diligence and compliance requirements related to all agents and business partners including (a) documented risk-based diligence and (b) informing agents of the Company’s commitment to abiding by the law; and
- Include standard provisions in agreements, contracts and renewals of all agents and business partners pertaining to anti-corruption, including anti-corruption representations and undertakings, rights to conduct audits, and rights to terminate as a result of any breach of anti-corruption laws and regulations or representations and undertakings.

Collusion and Management Override
Even the best anticorruption entity and transaction-level controls might be vulnerable to potential collusion, management override or other circumvention. To mitigate this risk, the remediation analyses should also assess whether management in the targeted areas have “bought in” to an effective anti-corruption program. Interviews of these individuals and their direct reports are often useful in assessing future risks. Compliance should be built into the compensation, goals and evaluation process of country and regional managers. The remediation team should also assess the design of the controls, including compensation controls to guard against collusion and override and validate operating effectiveness to ensure that employees and third parties are complying with enhanced policies and controls.
Discipline
Companies 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.

Periodic 3rd Party Review
Remediation programs require periodic review to ensure the effectiveness of remedial efforts. Prompt and proactive action is essential, if the company is to avoid a government imposed compliance monitor or independent consultant. The DOJ and SEC consider various factors: (a) seriousness and duration of the misconduct; (b) pervasiveness across geographic and product lines, (c) ethics and compliance program prior to the misconduct and, of course, (d) quality of remedial efforts.22

Companies can beat the government to the punch by voluntarily installing its own monitor. This strategy works only if company’s monitor is highly credible and completely independent.

Incident Response & Remediation
Finally, an effective FCPA remediation must include a response plan if and when future allegations of corruption allegations arise. FCPA settlement agreements typically require companies to:

- Develop a process for responding allegations of violations of anti-corruption laws and
- Maintain mechanisms for making and handling reports and complaints related to potential violations of anti-corruption compliance issues, including a process for investigating and ensuring that appropriate remedial measures are undertaken.

* * *

FCPA allegations are akin to angina attacks. Respond appropriately and life continues as normal. Fail to remediate and the organization faces the corporate equivalent of a heart attack.

2 Id at 71.
4 Id.
8 Cf. Institute of Internal Auditors, International Standards for the Professional Practice of Internal Auditing §1130A.1 (2010)(internal audit cannot audit its own work)
11 USSC, Chapter Eight Fine Primer: Determining the Appropriate Fine Under the Organizational Guidelines 4 (2011)
12 COSO is an acronym for the Committee of Sponsoring Organizations of the Treadway Commission. Information about COSO is available at http://www.coso.org.
14 FCPA Resource Guide at 58.
15 Id.
16 Inherent likelihood and significance refers to assessing risk without regard to existing controls.
17 FCPA Resource Guide at 57.
18 USSG§8B2.1.
19 FCPA Resource Guide at 57.
20 Id.
21 Id. at 61 – 62.
22 Id. at 71.