Bloomberg Law

White Collar Crime Report™

CORPORATE COMPLIANCE

Two attorneys with Bass, Berry & Sims PLC examine red flags for companies with multi-jurisdictional operations. The authors explain the importance of identifying and analyzing these red flags, and when appropriate, remediation.

Mitigating Risk: Identifying, Remediating Anti-Corruption Red Flags

BY WALLACE DIETZ AND LINDSEY FETZER

Anti-corruption red flags are present in virtually any organization with multi-jurisdictional operations or touch points. Presence of a red flag does not mean that there has been a violation of law or compliance program failure. Rather, red flags are simply a suggestion of increased risk. What matters is that companies proactively seek to identify and analyze red flags, and when appropriate, remediate potential issues. Effective anti-corruption compliance programs should acknowledge the risk attendant to operating on a global scale and seek to minimize potential exposure and enforcement scrutiny; this includes proactively identifying and remediating anti-corruption (and other) red flags. This article explores how organizations can best mitigate anti-corruption risk through understanding, identifying, and where appropriate, remediating anti-corruption red flags.

Wallace W. Dietz is a Member with Bass, Berry & Sims PLC. Dietz, the chair of the firm's Compliance & Government Investigations (CGI) Practice Group, has more than 30 years of experience guiding his clients through complex litigation and investigations where exposure is significant. He can be reached at wdietz@bassberry.com.

Lindsey Fetzer is an associate with Bass, Berry & Sims and a member of the firm's CGI Practice Group. She can be reached at lfetzer@bassberry.com.

Identifying Red Flags

Early identification of a red flag allows for an organization to put a stop to problematic or high-risk practices before a pattern emerges. Examples of potential anti-corruption risk areas include:

(1) third parties;
(2) gifts, travel, and entertainment;
(3) hiring practices;
(4) political and charitable contributions;
(5) licenses and permitting;
(6) customs clearance; and
(7) weak accounting and internal controls.

The following are examples of compliance program elements used to identify the presence of risk indicators and red flags.

Risk Assessments

Risk assessments proactively evaluate an organization's baseline risk: they show an organization where to look for red flags. Typically, a risk assessment involves the identification of geographical and operational risk factors, including risk presented by business partners and third-party vendors or suppliers. Risk assessments also evaluate the strength and efficacy of an organization's internal controls. Understanding where normal risk lies allows organizations to design a targeted compliance program that effectively mitigates known areas

 ISSN 1559-3185

of exposure. These routine reviews better position an organization to quickly identify discreet red flags before they become systematic violations.

Employee & External Reporting

Employee reporting is the hallmark of any red-flag identification effort. Most companies mandate that employees report red flags. Reporting mechanisms should allow for confidential and—when not in conflict with applicable data privacy or other regulations—anonymous reporting of potential instances of red flags. Examples of mechanisms by which employees can report include:

(1) a hotline;

(2) an email or electronic report;

(3) communications to the general counsel's or compliance office;

(4) communications to direct report or other supervisor.

In addition to encouraging reports to be made by whistleblowers, companies should encourage its subsidiaries, vendors and other third parties to do so as well.

Routine Anti-Corruption Internal Audits

Red flags will not always be identified through a whistleblower tip or other reporting mechanism; oftentimes, the presence of red flags is only discovered through periodic monitoring and review, including through an anti-corruption internal audit. Anti-corruption audits seek to test the effectiveness of internal controls and identify red flags. They are proactive and ''routine,'' and are distinct from the transaction testing often performed as a component of a reactive investigation. Anti-corruption audits should be targeted and location specific. Audit locations should be selected based on the results of a risk assessment. Anti-corruption internal audits can either be standalone (oftentimes preferable) or as an integrated component of a larger internal audit. Most often, anti-corruption audits include some combination of transaction testing, interviews and other fieldwork, and an analysis of existing compliance program elements and internal controls.

What to do When A Red Flag is Identified?

If and when a red flag is identified, appropriate follow-up should be conducted. Based on the severity and credibility of a potential allegation, this could include some type of anti-corruption internal investigation. A properly scoped and conducted internal investigation can pay dividends to an organization. Examples of benefits of a properly conducted internal investigation include:

(1) early and accurate assessment of potential legal exposure;

(2) identification and, potentially, discipline of employees involved in misconduct; and

(3) enhanced credibility with enforcement authorities, including a demonstration of the company's commitment to compliance.

Not all internal investigations are created equal. The scope of an investigation should balance the need for an objective, thorough internal investigation against economic pressure to control costs. Successfully responding to and resolving a compliance issue through an internal investigation requires collaboration and support from personnel across many corporate functions. Consideration should be given to whether and when to involve outside counsel and, when appropriate, forensic accountants. Following an investigation, findings and remediation should be appropriately documented, and results analyzed and synthesized.

Conclusion

Global companies are conducting business in an increasingly sophisticated regulatory landscape with ever-evolving anti-corruption risks. Anti-corruption enforcement continues to be aggressive and coordinated. Companies need to be proactive in order to be appropriately reactive. Red flags must be detected early. Organizations should affirmatively seek to detect and remediate red flags vis-à-vis a well-functioning compliance program.

WCR ISSN 1559-3185