

RISK-BASED COMPLIANCE

A recent benchmarking survey of Third Party Codes of Conduct was conducted by the Society of Corporate Compliance and Ethics (SCCE) and reported on by Rebecca Walker. The findings indicated that a majority of companies with an otherwise robust compliance program do not extend this to third parties with which they conduct business. The findings revealed the following: 53% of companies do not disseminate their internal codes of conduct to third parties; only 26% require third parties to certify to their own codes; and just 17% of the respondents have any third party codes of conduct.

For those companies which now desire to evaluate their third party business partners for Foreign Corrupt Practices Act (FCPA) compliance, how, and perhaps where, do they begin? The approach that appears to be gaining the most traction both with regulators and learned commentators is to develop a risk based approach to FCPA compliance. There is no specific Department of Justice (DOJ) guidance on any one specific process for a risk based compliance system. However, there is sufficient guidance in other FCPA and analogous compliance areas, such that direction can be provided to US and foreign companies in this area.

Writing in the FCPABlog, Scott Moritz of Daylight Forensic & Advisory suggested that a risk-based approach based upon the regulatory programs in Anti-Money Laundering (AML) governance. In the AML areas, the concept is that certain parties, including vendors, represent a higher compliance risk than others. Geography, nexus to government officials, business type, method of payment and dollar volume - are all risk indicators.

This risk-based approach was commented upon, favorably by the DOJ, in Release Opinion 08-02. In this Release Opinion the DOJ reviewed and approved Halliburton's proposed acquisition of the UK entity Expro. The DOJ spoke directly to a risk based approach by that Halliburton had agreed to provide the following:

. . . a comprehensive, risk-based FCPA and anti-corruption due diligence work plan which will address, among other things, the use of agents and other third parties; commercial dealings with state-owned customers; any joint venture, teaming or consortium arrangements; customs and immigration matters; tax matters; and any government licenses and permits. Such work plan will organize the due diligence effort into high risk, medium risk, and lowest risk elements.

This risk-based approach has also been accepted by UK's Financial Services Authority (FSA) in its settlement of the enforcement action against the insurance giant AON earlier this year. As a part of the settlement AON agreed to the following:

AON...designed and implemented a global anti-corruption policy ... limiting the use of third parties ... whose only service to AON is assisting it in the obtaining and retaining of business solely through client introductions in countries where the risk of corrupt practices is anything

other than low. These jurisdictions are defined by reference to an internationally accepted corruption perceptions index. Any use of third parties not prohibited by the policy must be reviewed and approved in accordance with global anti-corruption protocols.

How does a company implement this guidance? Scott Moritz suggests that key to any risk-based approach is “the strategic use of information technology, tracking and sorting the critical elements -- including risk-ranking, as well as enhanced due diligence and ongoing monitoring of high-risk parties proportionate to their risk profiles.”

The uses of a risk based compliance system can be myriad. The Release Opinion 08-02 system was in response to an international acquisition. Such systems can also be used to rank and assist in the evaluation of business partners or supply chain vendors. But, however such a system is used, the clear import from the DOJ, FSA and learned commentators is that some type of rational system should be put in place and followed.