How do You Evaluate a Risk Assessment?

What is the amount of risk that your company is willing to accept? Before you even get to this question how does your company assess risk and subsequently evaluate that risk? In the July issue of the Compliance Week magazine, these questions were explored in an article entitled "*Improving Risk Assessments and Audit Operations*" in which author Tammy Whitehouse discussed the audit process and how the audit results can form the basis for the evaluation of a risk assessment. In her article Whitehouse focused on the presentation of Michele Abraham, from Timken Co., and how Timken assesses and then monitors risks it determines through its annual compliance audit.

According to Abraham, once risks are identified, they are then rated according to their significance and likelihood of occurring, and then plotted on a heat map to determine their priority. The most significant risks with the greatest likelihood of occurring are deemed the priority risks, which become the focus of the audit monitoring plan, she said. A variety of solutions and tools can be used to manage these risks going forward but the key step is to evaluate and rate these risks. Abraham provided two examples of ratings guides which Whitehouse included in her article. We quote both in their entirety.

LIKELIHOOD

Likelihood Rating	Assessment	Evaluation Criteria
1	Almost Certain	High likely, this event is expected to occur
2	Likely	Strong possibility that an event will occur and there is sufficient historical incidence to support it
3	Possible	Event may occur at some point, typically there is a history to support it
4	Unlikely	Not expected but there's a slight possibility that it may occur
5	Rare	Highly unlikely, but may occur in unique circumstances

'Likelihood' factors to consider: The existence of controls, written policies and procedures designed to mitigate risk capable of leadership to recognize and prevent a compliance breakdown; Compliance failures or near misses; Training and awareness programs.

PRIORITY

Priority Rating	Assessment	Evaluation Criteria
1-2	Severe	Immediate action is required to address the risk, in addition to inclusion in training and education and audit and monitoring plans
3-4	High	Should be proactively monitored and mitigated through inclusion in training and education and audit and monitoring plans
5-7	Significant	
8-14	Moderate	
15-19 20-25	Low Trivial	Risks at this level should be monitored but do not necessarily pose any serious threat to the organization at the present time.

Priority Rating: Product of 'likelihood' and significance ratings reflects the significance of particular risk universe. It is not a measure of compliance effectiveness or to compare efforts, controls or programs against peer groups.

At Timken, the most significant risks with the greatest likelihood of occurring are deemed to be the priority risks. These "Severe" risks become the focus of the audit monitoring plan going forward. A variety of tools can be used, such as continuous controls monitoring with tools like those provided by Visual RiskIQ, a relationship-analysis based software such as Catelas or other analytical based tools. But you should not forget the human factor. At Timken, one of the methods used by the compliance group to manage such risk is by providing employees with substantive training to guard against the most significant risks coming to pass and to keep the key messages fresh and top of mind. The company also produces a risk control summary that succinctly documents the nature of the risk and the actions taken to mitigate it.

The key to the Timken approach is the action steps prescribed by their analysis. This is another way of saying that the risk assessment *informs* the compliance program, not vice versa. This is the method set forth by the US Department of Justice (DOJ) in its Compliance Program *best practices* and in the UK Bribery Act *Adequate Procedures*. I believe that the DOJ wants to see a reasoned approach with regards to the actions a company takes in the compliance arena. The model set forth by Michele Abraham of Timken certainly is a reasoned approach and can provide the articulation needed to explain which steps were taken.

purpose, provided attribution is made to the author. The author can be reached at tfox@tfoxlaw.com.