COSMOS
Navigate the Compliance Universe

CEP Magazine - April 2022
Do we have one risk or ten?

By Gerry Zack

Please feel free to contact me anytime to share your thoughts: +1 612.357.1544 (cell), +1 952.567.6215 (direct), gerry.zack@corporatecompliance.org.

- twitter.com/gerry_zack
- linkedin.com/in/gerryzack


Gerry Zack

As usual, Joe Murphy wrote an excellent column this month dealing with risk assessments.[1] We must be leading parallel lives, because I also had an idea about risk assessments I wanted to share.

Most readers use some variation of the same model for risk assessments, involving identification of risks, assessing severity via measurements of likelihood and impact, and measuring the mitigating effect of internal controls over compliance, resulting in some form of "net" or "residual" risk that is compared to a target level of risk. Often, the identification of risk results in categories of risks, such as bribery, loss of personal data, antitrust, etc.

This approach is usually just fine for these early stages of the risk assessment. But at some point, it is important to consider the different manners in which each of these categories of risk could occur. What starts out as one risk now may appear to be many more risks once this is done. It is critical to do this, since the internal controls needed to mitigate the risk can differ significantly from one to another. This is known as going from a risk category to the spectrum of risks within that category. It can be done at the risk identification stage, but must happen no later than the step during which the effectiveness of existing internal controls is being considered.

Consider the example of the risk that your company could pay bribes to a government official to win a contract. This might start out as one category of risk. But think about how many ways in which this bribe transaction could occur. I once came up with a lengthy list of more than 10 very different methods of paying bribes. The list included techniques such as setting up shell companies through which bribes would be funneled; establishing ghost employees in the payroll system; having salespeople or sales agents directly pay the bribes, which then show up on expense reports or vendor invoices; and convincing existing vendors to assist in getting the bribe to the official by inflating their invoices to us. More importantly, the internal controls necessary to mitigate each of these differ dramatically.

The only way to measure risk or to mitigate risk, when the risk can occur in many different manners, is by doing this type of analysis.

1 Joe Murphy, "Risk assessment: Thinking inside the box," *CEP Magazine*, April 2022.