COSMOS
Navigate the Compliance Universe

# CEP Magazine - January 2020
# Third-party due diligence red flags: Now what?

By Mariette Cutler, CFE

**Mariette Cutler** (mariette.cutler@gmail.com) is Managing Director of Risk Navigation Group Inc. in Chicago Illinois, USA.

Well-designed compliance programs should apply risk-based due diligence to their third-party relationships. The main takeaway from the DOJ guidance[1] is the word "risk-based." Risk is part of doing business, and eliminating too much of it can hamper company growth. Even if you invest an unlimited amount of money, time, and energy into a due diligence program, you can never eliminate all risks, including third-party risk. There is no one-size-fits-all approach to mitigating this specific type of risk, but there are some things to keep in mind when a red flag does show up in the due diligence process. A red flag does not mean per se that a company cannot do business with the third party; it means does the company want to do business with this third party, given the red flag?

## Screening for red flags

Each red flag will have specific, but sometimes limited, information available to base the decisions on. The more information that can be used to screen the third party, the more accurate the results will be. Once a third party is screened, the first step will be to analyze the information that the screening provides, such as:

- **Third party's name:** Does the name match fully or is there merely a fuzzy match. Do not discount aliases, but ensure that the red flag is indeed the third party that was intended to be screened.
- **Location:** Is the screened third party located in the same place as the red flag? Sometimes there will be a match in name, but the third party is flagged in a different country. This tends to happen with common proper names that are screened.
- **Nature:** What event caused the red flag? If the third party was convicted of money laundering and served time in jail, they may not be the best finance consultant of an overseas operation with limited oversight. However, if the third party is related to a politically exposed person (i.e., someone whose prominent position may make them more susceptible to bribery or corruption), there may be simple and effective controls in place to ensure the risk is limited.
- **Time frame:** When did the cause of the red flag occur? Was it a 20-year-old case that is irrelevant to today's business, or is it a politically exposed person within the last six months? The recency of the red flag event should be considered as part of the overall analysis.
- **Full company/single division:** Does the red flag indicate that there is trouble on the corporate level and throughout all divisions, or was it a single event at a specific division?
- **Business relationship:** What is the business rationale for the third party? In case of a sole-source supplier, there may be few or no alternatives. However, in the case of commodities, alternative suppliers could be considered.

The risk analysis phase in the due diligence process will identify: (1) false positives that can be ignored, (2) red flags that are true but not applicable to the specific situation, and (3) red flags that should be evaluated further. As the due diligence program matures, the algorithm should be refined and improved to reduce false positives. These are a waste of valuable time that could be spent on investigating red flags that are true warning signs. Those are the red flags that require the business to decide whether to move forward with the third party that got flagged or find an alternate business partner. The business decision will come down to the acceptable level of risk.