**MEMORANDUM – 2 MINUTE BRIEFING 4**

**TO:** CASEY G. CEGIELSKI, PH. D, CISSP, CISA, CRISC

**FROM:** CENSORED

**DATE:** 9/23/19

The two types of Risk Assessments available to your business are quantitative and qualitative; the first is used to calculate absolute financial values, while the latter just calculates relative financial values. The first type of risk assessment may be the preferred option since it will identify the priority of risks and the effectiveness of controls through establishing financial values for everything. The issue with this risk assessment is that accurate data isn’t always available and some additional steps may need to be taken to ensure that employees use the control as expected. The second type of risk assessment will determine the same results as the other: the probability of a threat exploiting a vulnerability and the determined impact as a result of it. The difference lies in the fact that this one does not determine absolute financial values like the other one; rather, this type of risk assessment uses the opinions of experts and is therefore much easier to complete. The issues that come with this type of risk assessment are exactly what you would expect: it’s subjective (since it is based on the testimony of experts, the value of the assessment is only as valuable as the expertise of the experts) and there are not really any standards for the outcome of this risk assessment.

No matter what type of risk assessment you choose to go with, you will need a schema for addressing risk levels. A schema is important because it helps visually map out levels of risk for certain areas and associated consequences of a threat exploiting the risk. A schema must be designed for any risk assessment so that specific findings can be plotted; it can be used later when addressing the listed risks so that your business knows which ones to target first. If a schema is not used with a risk assessment, it would be much harder to determine what needs to be dealt with first (because people need to see the data visually plotted instead of just a wall of text/data). Based on the information I have provided to you, it is now up to your company to determine which type of risk assessment is the best fit. As a good rule of thumb, it might be better to do a qualitative risk assessment instead of quantitative, since numbers can sway the company opinion in dangerous ways and stray the focus away from minimalizing risk.