KnowBe4
Human error. Conquered.

KCM GRC: Risk Likelihood and Impact Scoring

In evaluating the various methodologies for risk assessment, there are effectively two categories: quantitative and qualitative. Staying true to the positioning of KCM as a simple to use GRC platform, a qualitative approach was taken. This also aligns with NIST 800-30.

A qualitative approach has both pros and cons, as does most everything in methodologies. The pros include: less time and staff resources, identification of higher risk without significant cost, and risk ranking by priority.

The cons of a qualitative approach are that results can be subjective, and the method does not factor monetary measures.

A traditional qualitative approach to scoring is having a 5 point scale for both likelihood and impact. Likelihood x impact = score. The issue with a linear point scale, is that the differences between risk scoring can be relatively minor but pose a much higher risk to the organization.

This led us to the Fibonacci sequence. With the use of the Fibonacci sequence, we place higher value as the uncertainty and complexity of a risk increase. This allows users to depict the risk in more significant value terms.