Risk Scoring Methodology

RiskWatch

1-800-360-1898 1237 N Gulfstream Ave. Sarasota, FL

www.riskwatch.com

Risk Scoring Methodology

Risk scoring is the process of attaining a calculated score that tells you how severe a risk is, based off of several factors. Without a standard model for risk scoring, risk and security teams would continually struggle to communicate internally about how to allocate resources appropriately in order to minimize costs and impact to business.

When considering risk scoring, methodologies typically fall into quantitative or qualitative. These two types can simply be broken down into whether the data is numerical, or it is not. Numerical data is quantitative, and qualitative data is more explanatory.

Quantitative Methodology

Quantitative analysis depends on assigning monetary values to risk components so you're purely working with numerical figures. In quantitative risk assessments, you use available data to reach a numerical value that can then be used to determine probability of a risk event and how much money is at stake.

Typical Formula:

Annual Loss Expectancy – Single Loss expectancy * Annual Rate of Occurrence = Financial risk per year for that asset.

This is your risk. This can be compared to other assets to prioritize mitigation tasks and to determine ROI for controls. Clearly, you do not want your annual cost of the control to exceed the Annual Loss Expectancy of the asset.

To help you with your risk formula:

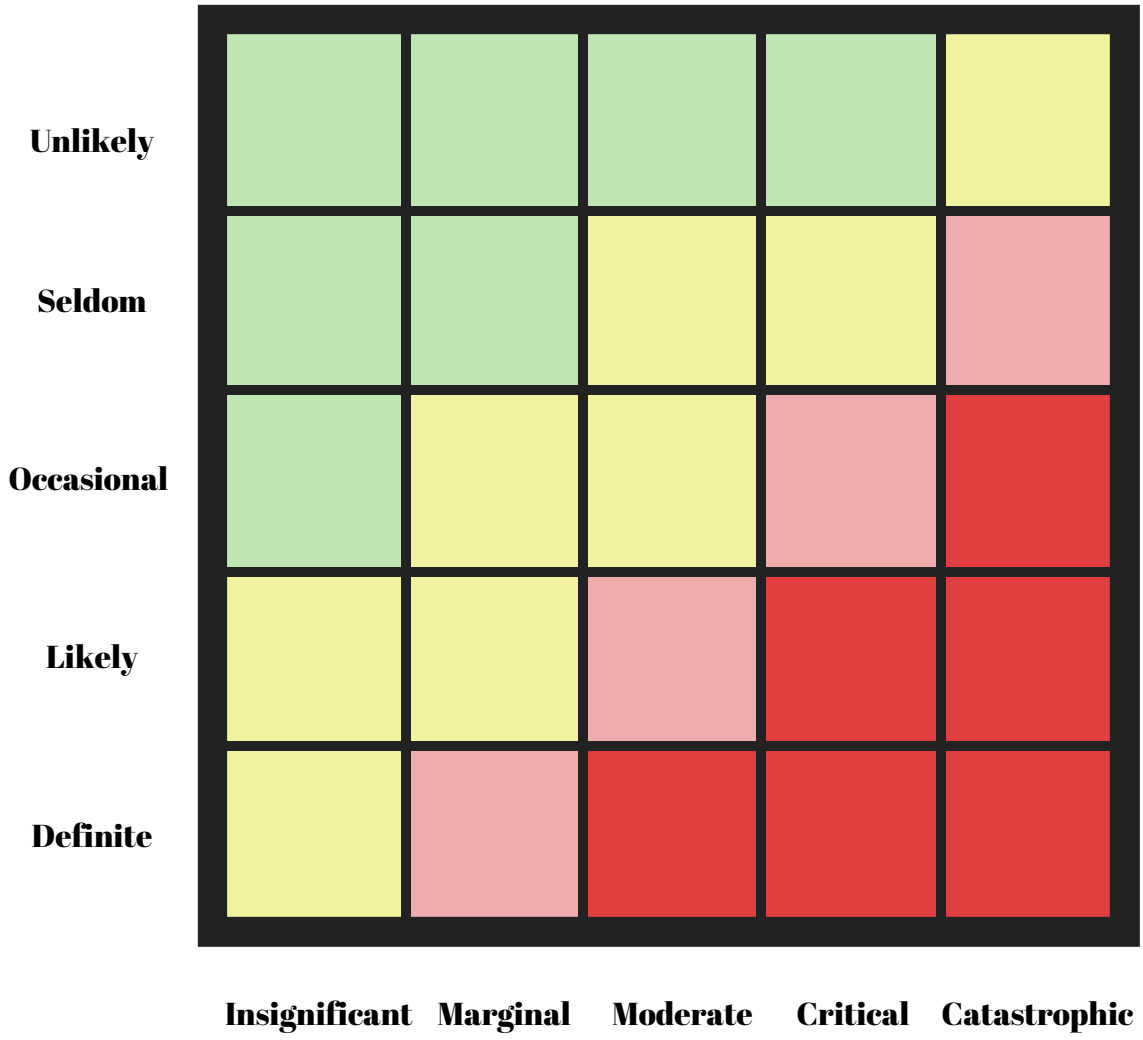
Single Loss Expectancy (Asset Value * Exposure %) – If the asset is compromised, how much $ will you lose?

Annual Rate of Occurrence (ARO) – How often do you expect the asset be compromised each year? (It is often a decimal. Once every 10 years equals .1 for ARO)

Qualitative Methodology

Qualitative analysis gives you more freedom in your rating and typically utilizes a Risk Assessment Matrix (RAM). It uses a more subjective assessment of risk occurrence likelihood (called probability) against the possible severity of the risk outcome (called impact) to establish overall severity of a risk.

Sample Risk Assessment Matrix



When creating your grading scales, you'll have to consider your assessment. In one case, a high risk rating could mean a risk is likely to occur in a month, where as another instance it could mean the risk is likely to occur in a year. The scales are flexible and encompass many considerations that impact risk scores.

Defining scales is typically seen as the most difficult aspect of utilizing a qualitative methodology.

RiskWatch Risk Scoring Methodology

RiskWatch employs a risk scoring methodology in our software that is best described as semi-quantitative. It's a methodology based on the philosophies of Hazards President, Fred A. Manuele, presented in his book "Advanced Safety Management."

> Fred A. Manuele, CSP, PE, is President of Hazards, Limited. He was awarded the honor of Fellow by the American Society of Safety Engineers, inducted into the Safety and Health Hall of Fame International, and given the Distinguished Service to Safety Award by the National Safety Council.

RiskWatch software uses 4 factors when calculating a risk or compliance score. The definition of these factors can vary based on the product being used.

For example, SecureWatch, which focuses on physical security, employs these four factors:

- **Threat Level** (related to likelihood, based on the level of crime in the area, environmental volatility, history of terrorism incidents in the region, etc.)
- **Criticality** (importance of the facility to the organization as a whole)
- **Gap Score** (level of vulnerability based on the lack of security controls)
- **Consequence** (related to Impact, based on the potential losses - monetary, reputational, regulatory sanctions, etc.)

> Our Formula:
>
> **(Threat Level + Criticality + Gap Score) x Consequence = Risk**

Subjectivity in Risk Scoring

There a wide array of opinions on this topic, but RiskWatch is of the belief that there is no way to completely eliminate subjectivity in risk scoring. Yes, even with a fully quantitative methodology. Despite looking at historical data, there is still subjective input on the numerical value assigned to certain events or risk factors.

As Manuele states, "There are no universally applied rules to assign value to elements to be scored. Value numbers in all numerical risk scoring systems are judgmental and reflect the experience and views of those who create a system."

How do work to eliminate subjective risk scores? We allow you to set up universal scoring across departments, for example, determining monetary loss as consequence. Between departments, importance would be determined at the executive level, limiting subjective influence to a single source or group that allows consistent scores and comparisons.

The main benefit to our risk score methodology is the simplicity. You can gather accurate data that is easy to understand and work with. Most executives want a simple understanding of their organization and how resources are being distributed, with clear explanation.

Some Key Points in How We Created Our Risk Score Formula

“Historically, frequency of exposure has been one of the elements considered to determine event probability. However, giving frequency of exposure its own multiplier, separate from and in addition to a probability multiplier, diminishes the necessary emphasis on the severity of harm or damage that could result from the event.” As such, we include frequency as a compnenet of threat level.

A three or four-factor risk scoring system can distort or dilute severity level of a particular risk **if all three or four factors are given equal weight.** In Manuele’s writing, he gives an example of a poorly devised risk formula where an event with the highest level of severity (death) and a likelihood of occurance of 50/50 in a given year, did not produce a high score because other factors were also included that were given an equal weight to that of severity.

Multiple factors can be used separately, “provided that adequate weighting is given to severity of outcome in the scoring system.” You'll see that we utilize multiple factors by giving unique weight to each of the four factors in our risk scoring formula.

Severity should receive a 50% weighting to reflect the impact severity has on incident outcomes. In Manuele's sample equation, the rating for occurrence probability and rating for frequency of exposure are added together and then multiplied with severity.

Severity x (Probability + Frequency of Exposure) = Risk

Questions?

Reach out to us at support@riskwatch.com if you would like more clarification on our risk scoring. We offer free trials of our software so you can see our scoring firsthand and understand why consistent use of our software improves your liklihood of succesfully managing risk.