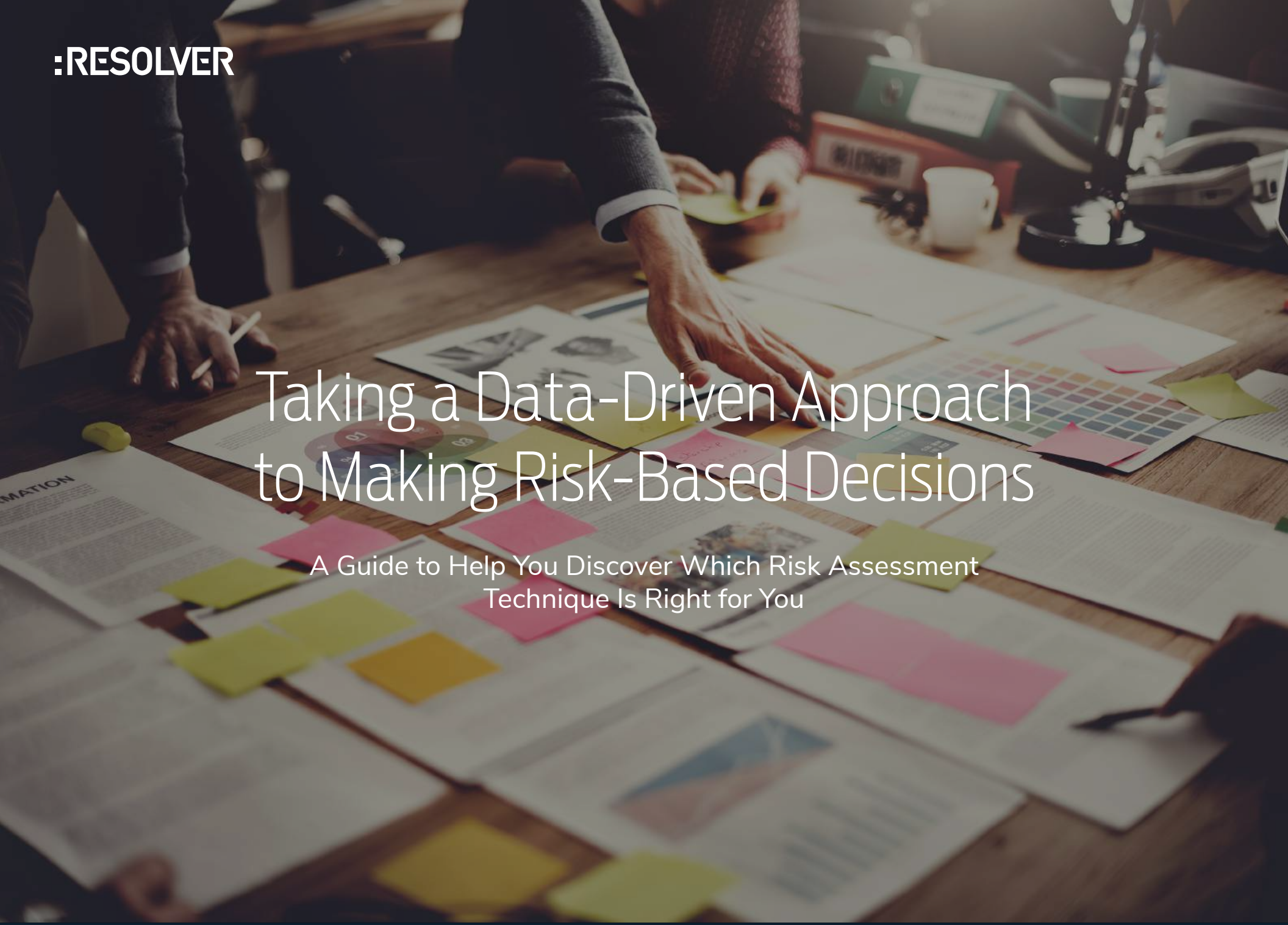
:RESOLVER



Taking a Data-Driven Approach to Making Risk-Based Decisions

A Guide to Help You Discover Which Risk Assessment Technique Is Right for You

Whether or not you want to admit it, your company faces risks every day. Every business does.

But how do you plan for risks—and when you're facing multiple threats, which ones are most important?

The easiest way is to guess. We humans do it all the time. Should you take Main Street or First Avenue home? Well, First is usually busy this time of night, so Main it is. Except—whoops, there's construction on Main, and now you're stuck in a traffic jam.

The thing about guessing is this: we like to think it works, but the reality is that it's a mental shortcut that is, at best, based only loosely on what happened in the past.

Because at the end of the day, our guesses just aren't very good. We're biased, and forgetful, and a thousand other things.

So how can we improve our ability to guess when it matters most—in other words, when we're making a risk-based decision?

By using data and foundational information to drive a risk assessment.

Risk assessment: three qualitative approaches

Qualitative risk assessments based on subjective criteria are effective when there is no relevant data present.

The three approaches below are typically used to assess strategic risks that have never occurred before.

Impact scale

Risks can be quickly rated on their potential impact. This is usually done with a 5-point scale that ranges from, for example, low to high, incidental to extreme, or very low to catastrophic.

These definitions are quantitatively defined so that the ratings mean the same no matter who uses them.

Figure 1 shows a typical Impact Scale.

Figure 1:

Rating	Definition
Extreme	• Financial loss of $X million or more • International long-term negative media coverage; game-changing loss of market share • Significant prosecution and fines, litigation including class actions, incarceration of leadership • Significant injuries or fatalities to employees or third parties, such as customers or vendors • Multiple senior leaders leave
Major	—
Moderate	—
Minor	—
Incidental	• Financial loss up to $X million • Local media attention quickly remedied • Not reportable to regulator • No injuries to employees or third parties, such as customers or vendors • Isolated staff dissatisfaction

Frequency scale

A frequency scale measures two factors: **frequency** (ranging from rare to frequent, for example), and **probability** (the likelihood of a risk occurring).

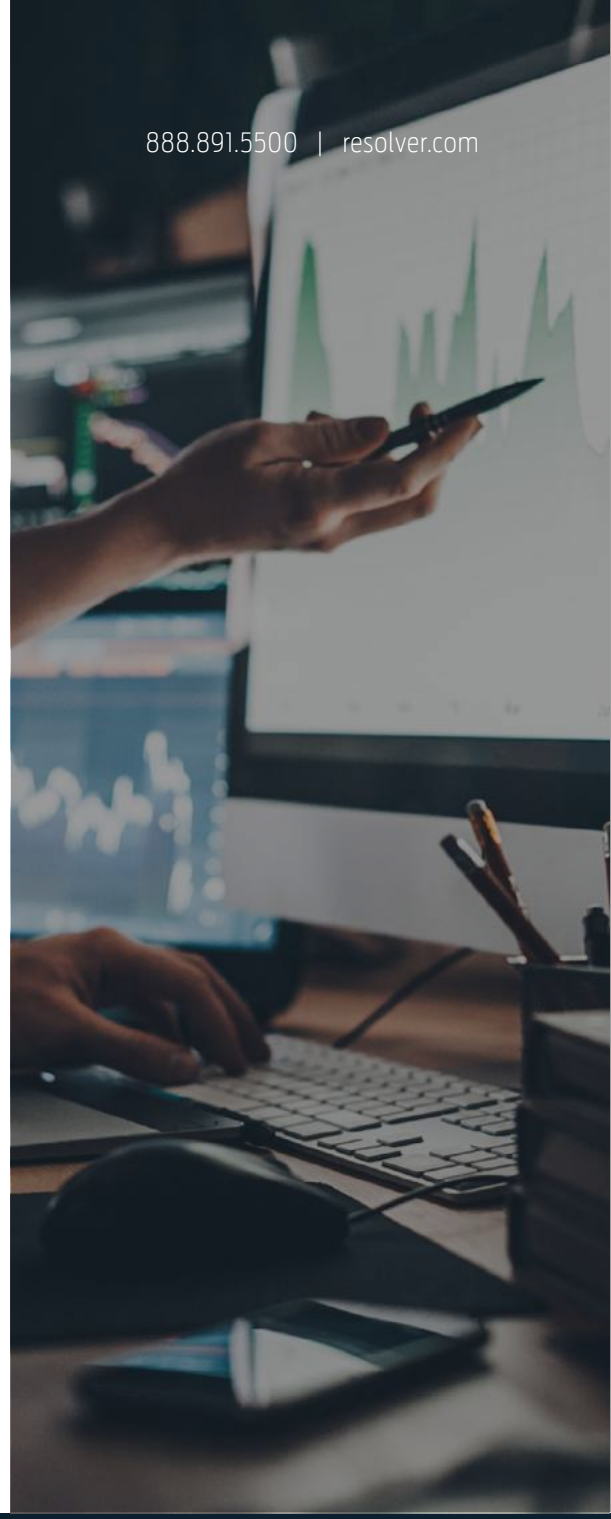
Quite often, frequency will be assessed within the context of a planning cycle—"What are the risks to our objectives in the next three years?"—or annually.

Like a qualitative risk assessment, this also is quantitatively defined so that the ratings mean the same across the board.

Figure 2 shows a typical Frequency Scale.

Figure 2:

Rating	Definition	Probability in life of asset or project
Frequent	Up to once in 2 years or more	> 90%
Likely	Once in 2 years up to once in 25 years	65%-90%
Possible	Once in 25 years up to once in 50 years	35%-65%
Unlikely	Once in 50 years up to once in 100 years	10%-35%
Rare	Once in 100 years or less	<10%



Vulnerability scale

Finally, a vulnerability scale assesses how well prepared we are for a risk event, ranging from very low vulnerability to very high.

Figure 3 shows a typical Vulnerability Scale.

Figure 3:

Rating	Definition
Very High	• No scenario planning performed • Lack of enterprise level/process level capabilities to address risks • Responses not implemented • No contingency or crisis management plans in place
High	—
Medium	—
Low	—
Very Low	• Real options deployed to maximize strategic flexibility • High enterprise level/process level capabilities to address risks • Redundant response mechanisms in place and regularly tested for critical risks • Contingency and crisis management plans in place and rehearsed regularly

Improving qualitative assessment

One way to understand how risk is part of a larger system—and thus understand and plan for it better—is a risk bow-tie. (Figure 4)

Figure 4:

Looking at the left-hand side of the bow-tie helps us understand the things that lead to a risk event, or influence the likelihood of the event occurring. The right-hand side describes the potential results of the event, which means it helps us understand the impact of that event should it occur.

A bow-tie is a useful tool because it helps you collect data, then add that data to your inputs and outputs to help you better assess likelihood and impact. Ultimately, this allows you to increase the accuracy of your risk assessment.

For example, let's say you want to learn which employees are gaining access to a restricted area. You could monitor access control behavior to see which rooms employees try to access, and find out how often employees end up in areas that they're not supposed to be in. These data points are typically referred to as Indicators or Key Risk Indicators (KRIs). Indicators typically have a target value—and when that threshold is crossed, an alert is issued to the appropriate person.

Using a bow-tie, you can focus on putting controls in place to mitigate or limit contributing factors, influence the flow of events, and alter the likelihood or impact of a risk.

In our example, you might run programs to improve employee morale, put restrictions in place to prevent unauthorized access, have asset redundancy to prevent service downtime, or use encrypted data to reduce the chance of IP theft.

Data-driven risk assessments

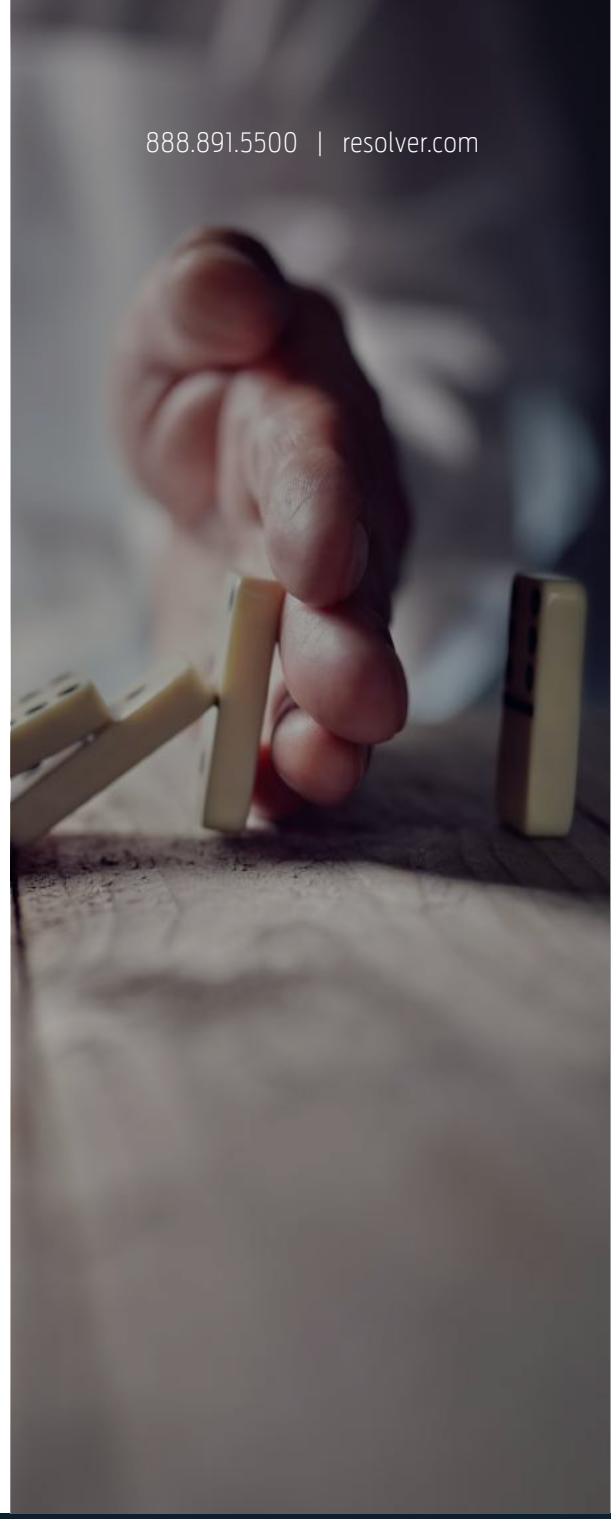
Qualitative risk assessments are better than nothing. However, each method is subject to bias and errors in estimation.

To improve your qualitative assessments, think about what data you have available, and about how you can use it for risk assessment.

You already know what the risk is, so what data will help you better monitor the risk or assess its impact? What event would take you off your target? How would you know if you were off-target, and what might indicate that you were off?

You can get a better handle on risk by mining through your data and looking for patterns or anomalies. In other words, data can be the greatest discovery tool for risks, helping you identify and assess the greatest risks to your organization.

However, because data needs to be interpreted and aligned to risk events, it's most effective when you have an incident data set that can be analyzed by a subject matter expert.



Four requirements for data-driven/incident-based risk assessments

You'll need four things if you'd like to start exploring the world of data-driven risk assessments:

1. **Risk events that are frequent enough to produce data.**
   You don't need huge numbers, but the more you have, the better. It's very hard to use an incident to predict a risk that is rare (such as a competitor releasing a similar product around the same time), but you could use it for a highly frequent event like a slip and fall. Reducing this risk still has a big impact, and it's something you will have enough data for.

2. **Risk events where the past is representative of the future.**
   Is it a representative model? There could be events that occurred in the past that are now irrelevant. For example, your old slip and fall data won't mean anything if your office is now in a different location than it was previously.

3. **Access to the data.**
   Do you have access? Can you get it? Sometimes this is hard because there are unknown or subjective factors.

4. **The ability to establish a baseline.**
   To do risk assessment right, you'll need data about when the risk didn't happen. For example, it's all well and good to analyze the 23 parking tickets your delivery drivers get in an average week—but what about the 900+ deliveries where they don't get ticketed? When you are looking to assess likelihood, you'll need to have some information to reference. The most obvious would be near misses—parking incidents that almost occurred, but didn't. Ideally, though, you'd look at the number of times a truck was parked illegally and didn't get a ticket, or perhaps even the number of times a truck was parked at all.

Takeaways

Start collecting data.

Remember to collect non-occurrences (near misses, total volume, times when controls worked). If you don't have the data, you can't use it to help you make informed predictions and assess risks based on data.

Use indicators and incidents to feed data into your models.

Look for the data you already have. How can you use it?

Consider Resolver.

Resolver software can help you with your risk assessment technique every step of the way. Define your scale and do a qualitative assessment, build a risk bow-tie so that you can understand the ins and the outs of the risk event, track key risk indicators around those things and feed data into the model, and use a standard process to quantify and assess the risks. Whatever it is, we can help.

Want to learn more? Let's talk.

resolver.com | info@resolver.com | 1-888-891-5500