ARCHER

EBOOK

Are You Getting the Most Out of Risk Heat Maps?

A Practical Analysis for Your Heat Maps

What do Risk Heat Maps Really Tell Us?

Using Heat Maps for risk management is an extremely common practice. The Heat Map is based on severity scores from a defined scale for likelihood and impact.

People use this approach to rank risks, plot them on a heat map, give some aggregate view of the portfolio of risks, and perhaps track the reduction in risk exposure as a result of any risk treatments that have been applied.

Using severity scores is more than just common practice, it is almost ubiquitous in the GRC world. Many times, these scores are one of the first stops on the risk management reporting curve. Risk teams first use Excel to create scoring models and then graduate to more sophisticated tools. No GRC software product is complete without them and the risks heat maps they can produce. But is it best – or even good – practice? And if it's not, what else can we use?

This eBook explores what heat maps can and can't tell us, and more importantly, how you can improve your approach to get on the path towards more precise risk quantification approaches.

This eBook:

1. Explains what a severity score is
2. Gives one of many possible illustrations of how severity scores can be more of a hindrance than a help
3. Shows you how to check for potential problems with your chosen heat map scoring rules; and
4. Explain how you can correct any issues.

What's a Severity Score?

A risk matrix, or risk heat map, is built up of **(almost always)** a 5 x 5 grid. On one axis is the likelihood of the risk, and on the other axis the expected impact. This makes pretty good sense, since the combination is the essence of how we think about evaluating a risk. A nominal 1-5 scale is applied to both likelihood and impact, and then they are multiplied together **(because risk is probability x impact – isn't it?)** to give a 'severity' score.

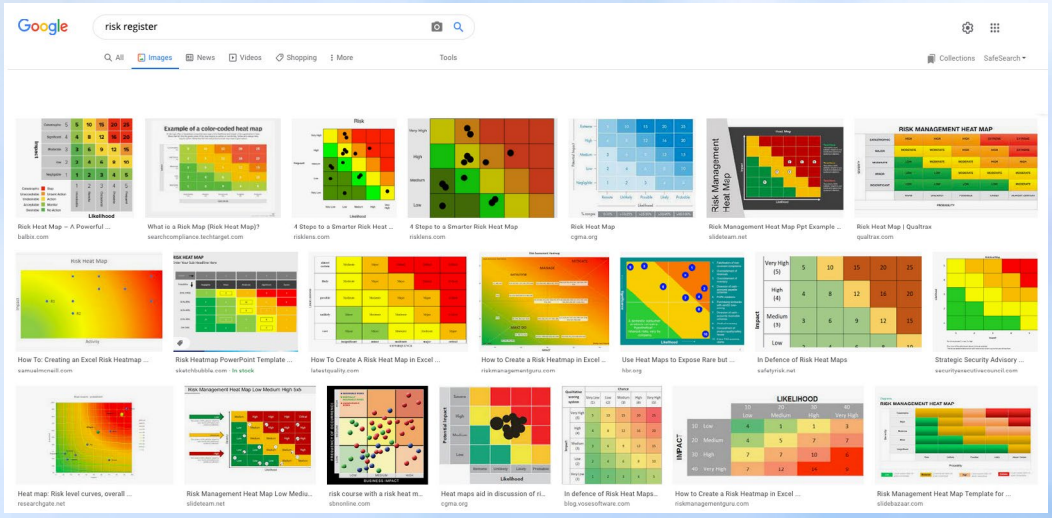
Likelihood						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
Severity =L x I		1	2	3	4	5
		Low	M Low	Med	Med H	High
		Impact				

Once we have a severity score, we can split up the 25 boxes into regions. Here, for example, there are three regions – green for insignificant risks, yellow for risks that are significant, and red for risks that are terrifying. Implicit in the traffic light coloring is:

- **Green** – don't worry
- **Yellow** – look at carefully
- **Red** – find ways to avoid

The result is a hierarchy:

Red is riskier than Yellow is riskier than Green. This traffic light color scheme is very popular indeed. A simple Google Image search for "risk register" results in all types of examples. The point is this approach has become ubiquitous in the discussion of risk at almost every organization.



Determining the Scale of Likelihood and Impact

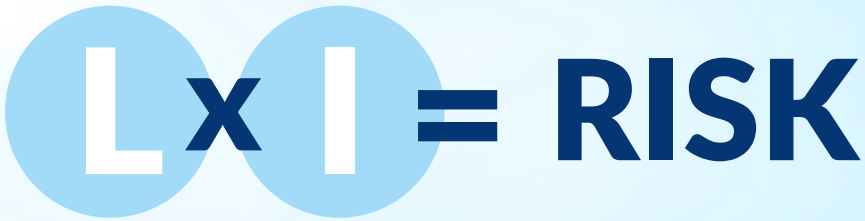
Getting started with risk heat maps is fairly straightforward. Hence, why the approach is so popular. Let's say you and I are joint owners of a multinational business worth $100 million and we are trying to evaluate some risks. First, we must set up our ranges for Likelihood and Impact so we can plot our risks on the heat map.

LIKELIHOOD

The Likelihood scale defines the probability a risk may occur. What I mean by a 'High' likelihood may not be the same as what you are thinking. Perhaps for you it's anything over 50%, and for me it's over 80%.

To avoid confusion, we should agree on a scale. We have five categories so let's split it evenly like this:

Likelihood	Score	From	To
High	5	80%	100%
Medium High	4	60%	80%
Medium	3	40%	60%
Medium Low	2	20%	40%
Low	1	0%	20%



IMPACT

The Impact scale defines the overall business impact if a risk event occurs. We also have the same calibration problem with impact. Logically, a High impact (a score of 5) can't be larger than $100M (since that is the value of our company), so let's split our impact scale evenly as well:

Impact	Score	From	To
High	5	$80M	$100M
Medium High	4	$60M	$80M
Medium	3	$40M	$60M
Medium Low	2	$20M	$40M
Low	1	>$0	$20M

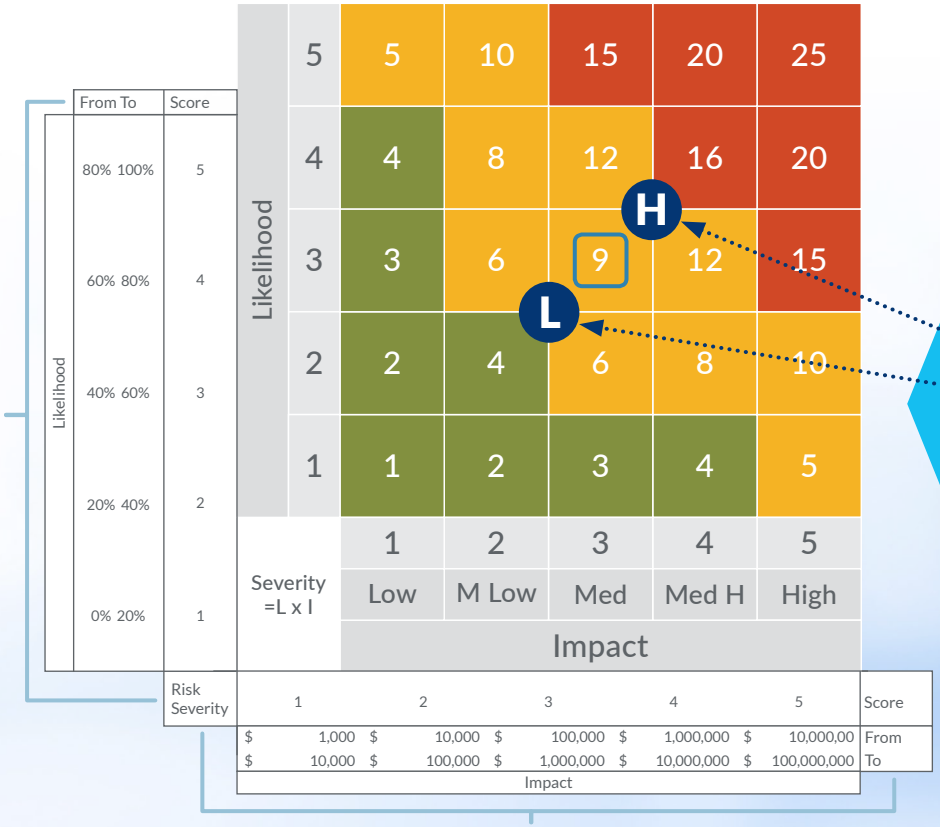
But that doesn't look right, does it? It is unlikely that a $10M loss could be called 'Low' for us, and we have hundreds of risks with very small impacts, we wouldn't want to bundle them together with $10M risks. We need to use another scale. Let's use a log scale:

Impact	Score	From	To
High	5	$10M	$100M
Medium High	4	$1M	$10M
Medium	3	$100k	$10k
Medium Low	2	$10k	$100k
Low	1	>$1k	$10k

Putting Numbers into the Heat Map

Now that we have our scales, we can go about putting numbers into our heatmap. Pretty much every company that has put bounds around likelihood and impact categories has arrived at a similar conclusion. There might be a bit of deviation, but the likelihood scale will be roughly linear and the impact scale roughly log. Let's build our heat map:

Likelihood	Score	From	To
High	5	80%	100%
Med. High	4	60%	80%
Medium	3	40%	60%
Med. Low	2	20%	40%
Low	1	0%	20%



A risk with medium likelihood (3) and medium impact (3) plots right in the middle of the grid with a score of 3 x 3 = 9. The dots on the corners help us figure out what this square means in monetary terms:

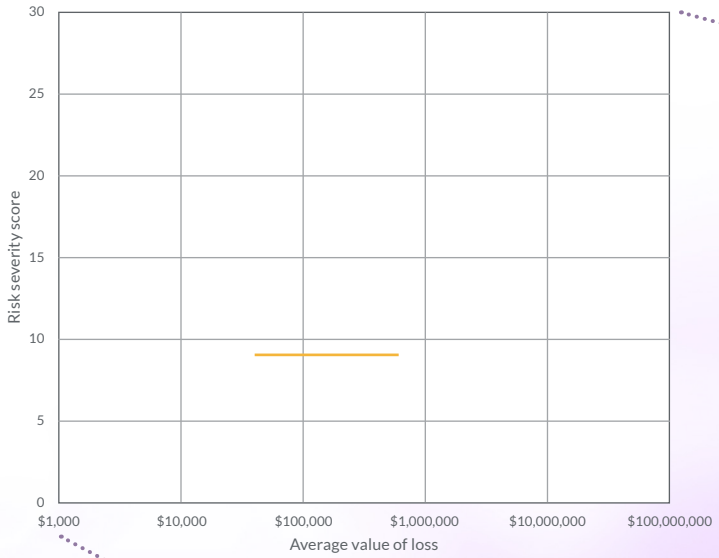
Corner	Likelihood	Impact	L x I
H	60%	$1M	**$600k**
L	40%	$100k	**$40k**

These figures represent the range of risks in this specific square.

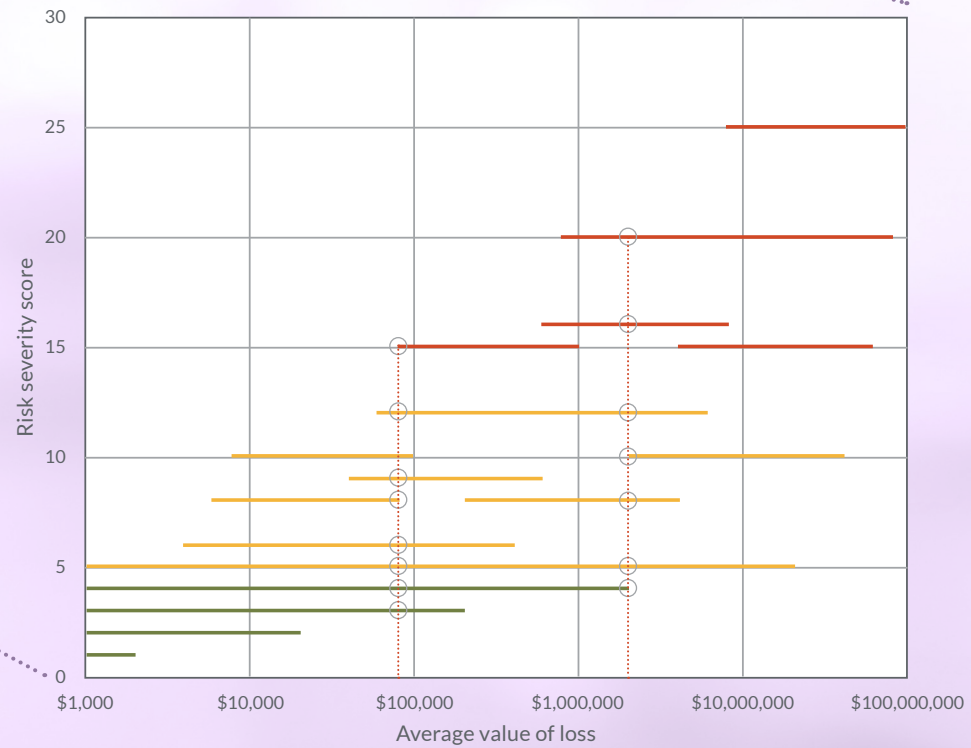
Impact	Score	From	To
High	5	$10M	$100M
Medium High	4	$1M	$10M
Medium	3	$100k	$10k
Medium Low	2	$10k	$100k
Low	1	>$1k	$10k

Ranges in a Heat Map

Now, let's plot the range for that square ($40k – 600k) on a graph, and color it yellow to reflect the heat map color. This gives us a visual representation of the overall range of one box in our heat map.



We can repeat the process for the other 24 squares, adding their lines to the graph:



See the problem? There is a huge overlap between the lines, so much so that, for example, a risk with an expected value of $80k (the left dashed line) could have a score between 3 (green) and 15 (red), and almost every other score in between.

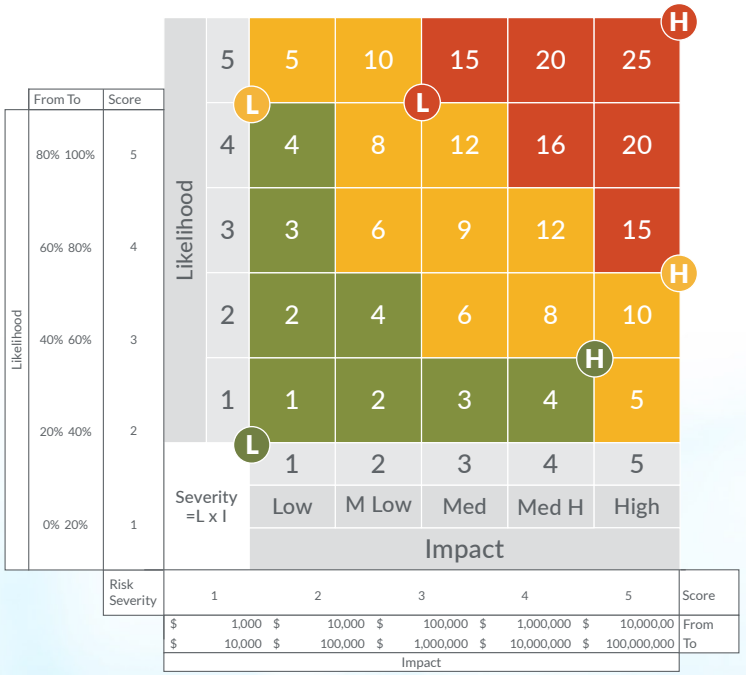
This graph illustrates the root challenge with utilizing a traditional risk heat map. With overlapping ranges, there isn't an accurate measurement of risk. While the heat map may spark good conversations, the lack of precision clouds decision making.

Check your own risk heat map

Are your reds worse than your yellows, and your yellows worse than your greens? Let's check if your risk heat map could be leading to wrong assumptions during risk discussions.

1. Draw out your heat map with impact on the horizontal axis, likelihood on the vertical – left to right is in increasing impact value, bottom to top in increasing probability.
2. Pick a heat map color.
3. Find the left most column in which that color appears. Find the lowest square in that column with that color. Note the likelihood and impact values associated with the bottom left corner of that square. Multiply them together. That's the lower bound for this color.
4. Find the right most column in which that color appears. Find the highest square in that column with that color. Note the likelihood and impact values associated with the top right corner of that square. Multiply them together. That's the upper bound for this color.
5. Repeat for the other colors.
6. Plot together the range each color spans and check for significant overlap.

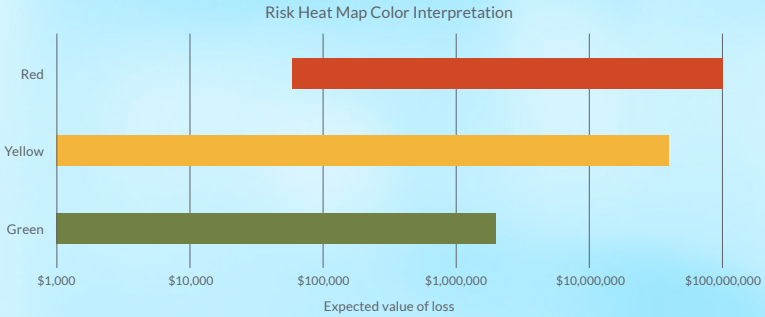
The points for each color in our example heat map are indicated in this illustration.



The calculations for these points give us the values in red:

	Low			High		
Color	L	I	L x I	L	I	L x I
Green	0%	$1k	$0	20%	$10M	$2M
Yellow	0%	$1k	$0k	40%	$100M	$40M
Red	60%	$100k	$60k	100%	$100M	$100M

Plotting these values for your heat map you can quickly check if there is a significant overlap. Using a log scale will make it easier to see:



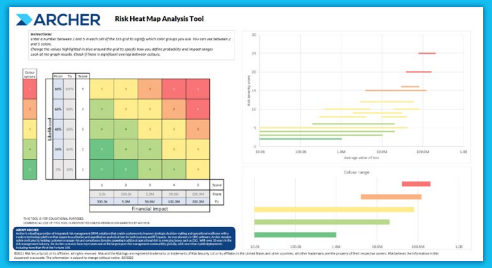
Recommendations

Risk heat maps are a tool to start the conversation around potential obstacles to business objectives. The imprecision outlined in this eBook could be hampering your decision making process. However, there are steps you can take to move towards a more meaningful analysis and more precise quantitative measure of risk.

- Try to avoid using bands for likelihood. Get a rough estimate of probability using numbers instead. Don't worry about being absolutely precise. Until someone invents a machine to measure probability, we are stuck with guessing. Your guesses will get better as you gather more information and become cleaner estimates. From Day 1, though, they will be a lot better than an arbitrary score or selecting from a wide range. For example, the chance of a meteorite destroying my house tomorrow and the chance of me crashing my car tomorrow are both "low", but we all know which one I should insure against.
- Use grids with likelihood and impact, just don't color them. Then you've turned the risk matrix into an x-y scatter plot. Use a log scale for both likelihood and impact, that way all risks with the same expected value will plot along an off-diagonal line and you can easily identify the largest ones.
- When you estimate the magnitude of a potential loss, consider the maximum (a) it could be, the minimum (b), and then the amount you think it would most likely sit around (c). A popular formula is then to use a loss amount equal to (a+b+3c)/5.

Once you have got this far, you have transitioned to fundamental risk quantification. You should be able to begin assessing aggregate exposures, consider cost-effectiveness of risk treatment programs, and have a more rational idea of the level of insurance cover you should purchase. You can start taking the right risks, avoiding the wrong ones, and use risk management as a strategic tool.

Assess Your Own Heat Maps



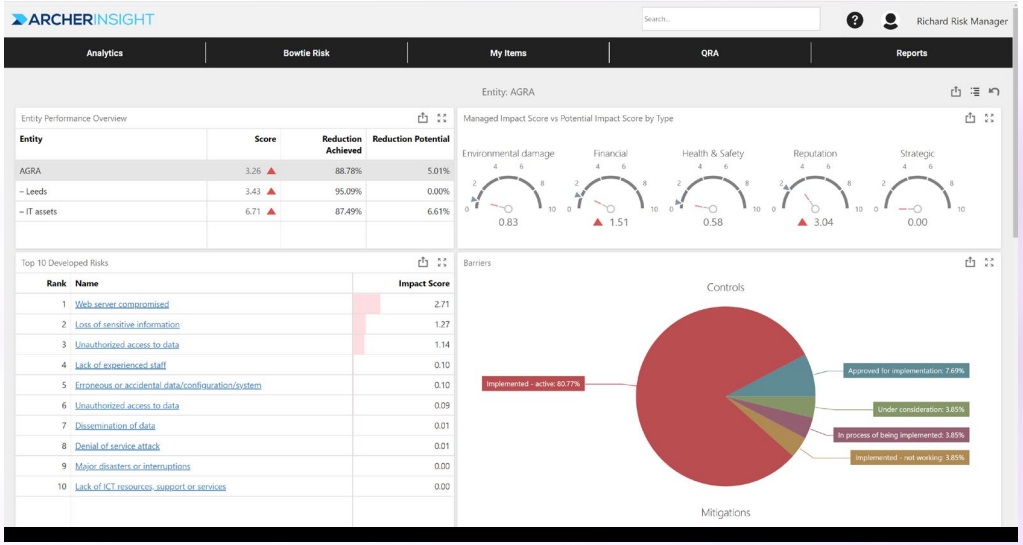
Download a tool to quickly assess your own heatmaps. Our simple Excel tool allows you to perform the analysis outlined in this eBook.

Download Tool

Archer Insight

Archer Insight is a suite of enterprise-wide risk quantification capabilities designed to deliver risk and business leaders a complete view of enterprise risks to improve resilience and ensure achievement of its strategic goals.

Our solution provides business leaders with more aggregated view of risks that allows them not only to ensure compliance but ultimately to better protect their business from disruption as well as address risks related to new opportunities. Using Archer Insight, organizations can conduct risk quantification analysis, monitor, and report on their risk management programs and then provide business leaders and decision-makers with quantitative, transparent, and actionable information needed to make strategic business decisions.



For more information, visit www.archerirm.com/archer-insight-risk-quantification

Archer Insight is entirely quantitative, enabling you to combine all the threats to your organization and truly understand the risks that matter. Our solution makes quantitative risk management quick and easy to use and provides a full set of tools and features for understanding and managing all types of risk in one platform: operational, project, cyber-security, health and safety, strategic and reputational risk.

Discover More

Archer is a leading provider of integrated risk management (IRM) solutions that enable customers to improve strategic decision-making and operational resilience with a modern technology platform that supports qualitative and quantitative analysis driven by both business and IT impacts. As true pioneers in GRC software, Archer remains solely dedicated to helping customers manage risk and compliance domains, from traditional operational risk to emerging issues such as ESG. With over 20 years in the risk management industry, the Archer customer base represents one of the largest pure risk management communities globally, with more than 1,200 customers including more than 50% of the Fortune 500.

Visit **www.ArcherIRM.com**.

@ArcherIRM Archer Integrated Risk Management

ARCHER