

Risk management textbooks, best in class presentations, white papers and standards etc., all identify that having a defined risk tolerance or risk appetite is pivotal for implementing a risk management process. Intuitively, it also makes perfect sense that you cannot validly discuss what is a big and a small risk, if you have not considered, what level of risk you are prepared to take.

However, when it comes to explaining or inspiring a risk manager on “how” to define a risk appetite and make this a tangible metric ... the textbooks and white papers and standards seem to fade out. There are very few explicit best practices – at least outside the financial industries - where risk management is essentially an operational pricing process.

Furthermore, risk appetite is by no means a static concept – just look at one’s personal level of risk appetite. Plenty of people enjoy riding a motorbike, even though it is known to be rather dangerous. Nevertheless, these same people, who choose to take the risk of driving a motorbike, systematically look for traffic before crossing a road, even when the level of traffic is limited and the risk of being hit by a passing car is small.

Most risk literature as well as the ISO 31.000 standard suggests that risk management operates with a series of concepts:

**Risk capacity...** The level of risk the company is based to bear without “dying” in the process. Exposure beyond this level is essentially “lethal” to the company.

**Risk tolerance...** The level of risk the company is prepared to take, including the effect of treatments, to meet its targets. This level of risk taking is not to be exceeded by any individual risk or the risk portfolio.

**Risk appetite...** The level of risk the company is willing to take and retain in pursuit of defined targets, and hence the level of risk, the company accepts without further mitigation.

Modelled, it may look as the below sequence of increasing risk exposure:



One may choose to operate with all of these, but you can get a strong implementation just focusing on one, and be quite assertive about what this is. As risk professionals, we have to be aware that management and the board of directors we are addressing are not risk management professionals; and are, hence, more prone to act on a simple and intuitively understandable concept than a combination of multiple metrics.

Below, it is assumed that we are working with the concept of “risk tolerance”, defined as the level of risk, the company is prepared (i.e. not necessarily willing) to take to prosper in their industry. We look at a basic approach and definition and a consolidated approach with a maximum limit to defining risk tolerance.

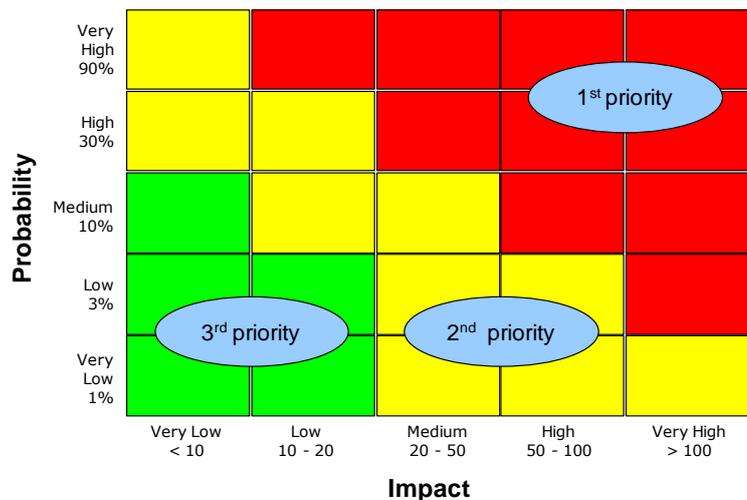
**A Basic Approach and Definition to Risk Tolerance**

As mentioned, the “how” to define a risk tolerance for a company is not a matter of general knowledge, and many companies have implemented rather comprehensive risk management processes without having explicitly defined a risk tolerance. However, it really need not be very complex. Adhering to the 80/20 rule, will give the company 80% of the value using 20% of the efforts.

The suggested first step is to actively use a defined risk map, which most companies apply “the minute” they start obtaining an overview of their risk exposure. Here, for strategic risks, the underlying assessments are often estimates and coarse calculations as they do not have sufficiently detailed data to make in-depth statistics.

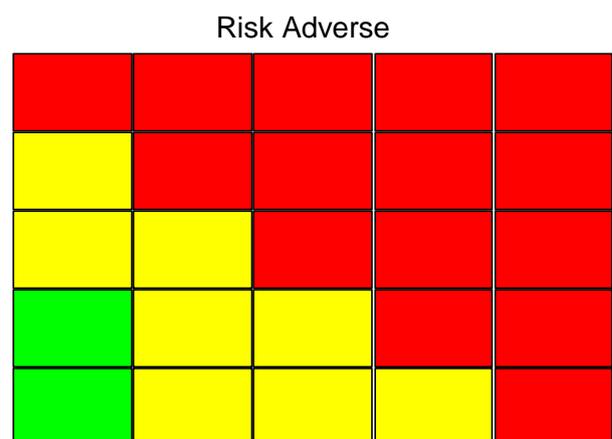
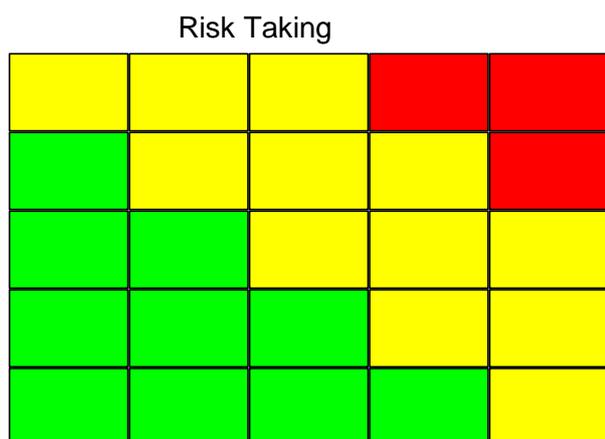
In this risk map, the probability and impact scales are defined explicitly--as they should be – and the cells have been color coded to indicate 1<sup>st</sup>, 2<sup>nd</sup>, and 3<sup>rd</sup> priority risks.

A company can now, define a risk tolerance in terms of: “We do not accept risks, which after mitigation, are still assessed to be 1<sup>st</sup> priority risks”. This limits the level of accepted net or residual risks to be those of 2<sup>nd</sup> or 3<sup>rd</sup> priority.



Furthermore, the scales can be used to define the risk tolerance. In this risk map it is stated that a very high impact is above 100 (e.g. million dollars), and the limits of the lower levels have been based on an approximate division factor of 2. These 100 million dollars may resemble, for example, projected earnings for the coming year, and hence essentially define the level of risk tolerance.

If/when the impact scale is “linked” to projected earnings this risk map becomes a dynamic expression of the exposure for the company. Higher earnings will lead to a more “aggressive” impact scale, whereas lower earnings will lead to a more cautious one. For example, an explicit risk with an impact of 70 million dollars and a 10% probability would be a 1<sup>st</sup> priority risk; but if the impact scale was “doubled” due to higher resilience it would be reduced to a 2<sup>nd</sup> priority. Beyond this, a company may choose different “designs” of risk maps. The below Risk Maps illustrates a risk-taking company and a more cautious/risk adverse company.



This basic approach is seen as intuitively understandable and provides management with a clear guidance as to the risk management efforts needed. Furthermore, the reporting of the net/residual risk exposure immediately documents compliance to the defined tolerance. However, it is not complete. A company can be severely exposed to risks by having a huge number of risks which are not or cannot be mitigated to a sufficiently low level. It does not, therefore, enable the measure of a “total” or consolidated exposure, which is the basis for the next step in working with a defined risk tolerance.

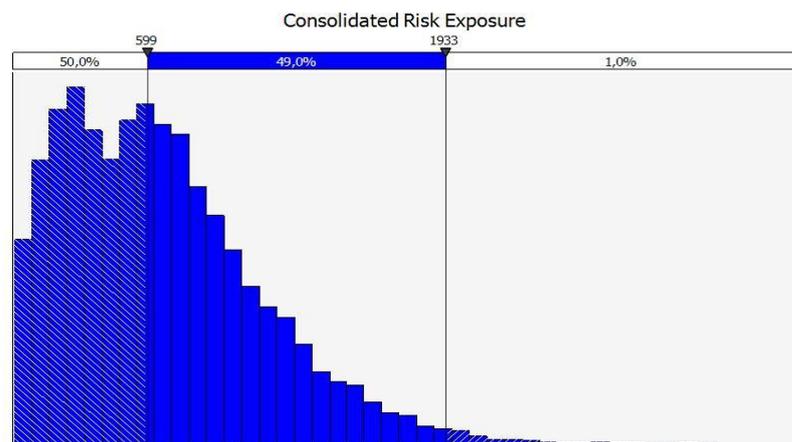
**A Consolidated Approach: Assessing Risk Exposure**

Risk management is about handling the extremes, where you cannot or will not live with the impact/consequences of the risk materializing ... irrespective of the probability. Referring back to the example of motorbike riding, if, whatever you do to drive carefully, still leaves a 1% risk of having an accident that damages your motorbike, and you cannot afford to lose it, you will have to insure the value of the bike – irrespective of how low the probability of such an accident is (or alternatively, refrain from riding in the first place).

It is frequently seen that companies consolidate risks by multiplying the probability of each risk with the impact of that risk, and then adding the portfolio up. This is a systemic error as it drives risk management into an issue of averages. If this were a valid approach, no-one would ever take out insurance on anything as the total costs of insurance premiums would exceed the average loss. (Insurance companies would be losing money every year.) Furthermore, one cannot validly add up the assessed impact of all risks in a portfolio as this inherently means that you assume ALL risks materialize at the same time. This is potentially not even possible. For example, if you lose your factory in a fire, it no longer has a consequence that a competitor limits your expansion into a new market.

Rather, one valid way to consolidate a risk portfolio is using Monte Carlo simulations. This is a mathematical technique where a computer is used to generate a huge number of “scenarios” based on the data provided and then compute the probability that outcome X will be higher than Y.

For example, the Consolidated Risk Exposure Chart, shows the result of such a simulation--- there is a 50% chance that consolidated losses will be less than 599 million dollars and the 1% worst case is a loss of more than 1.933 million dollars.

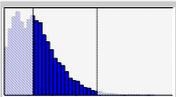


There are a number of rather simple software tools and add-on packages that can make this kind of consolidation.

When defining the exposure of a risk portfolio, there is the possibility of defining the statistic/stochastic distribution of each risk individually. Some will have a 1% probability of happening with the impact specified, and thus have a 99% probability of not happening, i.e. have a zero impact. Others will have a 10% probability that they happen once, 1% they happen twice, or 0,1% chance they happen three times. There are mathematical distributions that describe this well. In your risk

portfolio, you will need to define this for each risk, and then “run” the Monte Carlo simulation to get the results. See an example of a Monte Carlo simulation below.

As risk professionals, we have the mathematical background and insights to do these calculations and hence provide a valid consolidation of the risk exposure for the company. However, particularly for this reason, we should also be very cautious and recognize that no model can ever replace “common sense”.

Risk	Impact Mio USD	Probability %	Simulation
Competitor Move	80	30%	-
Loss of production capacity	200	3%	-
Failure to enter new market	50	10%	-
...			-
<b>TOTAL EXPOSURE</b>			

If a modeled calculation appears to be counter-intuitive, we have to validate our modeling before decisions are made. A key point to remember is that business trends follow simple logic more often than mathematical calculations.

### Assigning a Maximum Limit

Now that the consolidated risk exposure is made tangible and measurable, it makes sense to define a maximum limit that captures the essence of the company’s risk tolerance. This can hence be related to the metric on which the risks are assessed and defined in the risk map.

Assuming the impact scale is loss of profit compared to budget ... then the company risk tolerance can be defined as “*We do not accept that the net/residual risk exposure exceeds the budgeted earnings with more than 1% probability*” or “*We require a 99% certainty of a profit every year*”.

The degree of certainty must reflect the volatility of the industry. If the industry is highly volatile, one may find that a 99% assurance is either a larger than practical number, or essentially hampering management’s possibilities to develop and grow the company. The board of directors may then wish to use a 95% assurance. Such a metric is one that both management and the board of directors can understand and work with – without having to know the details of risk management terminology and mechanics. They have to assure themselves that they trust the underlying assessments and risk management processes.

### Non-financial risk taking

The above has been all about the money, but evolving the risk management approach, we have to face that an organization may be hampered by and vulnerable to a range on non-financial risks, where the risk tolerance has to be redefined. Some of these may be:

- Reputational      How much reputational “damage” do you accept as being your risk tolerance level. This may be measured in terms of press attention, negative social media attention, some image monitoring or the like.
- Environmental    How much environmental damage to your sites, and their surroundings will you be prepared to tolerate with mitigations.

Other scales may be safety, liquidity, collaborative trust, or whatever is pivotal for the company in question. The approach is the same, just applying other metrics and/or verbal descriptions to define risk exposure.

### Combining the Basic and Consolidated Approaches

I recommend implementing both of the above approaches, and hence using the “no 1<sup>st</sup> priority risks” definition of risk tolerance to ensure that no single risk severely jeopardizes the performance of the company AND using the consolidated figure to ensure that the exposure of the full portfolio is still acceptable.

### Benefits of a Defined Risk Tolerance

When management or the board of directors looks at the financial performance it is quite natural to compare this with the planned/budgeted performance and/or with the benchmark of other companies in a similar business. The outcome is an intelligent discussion of the performance, and how this can be sustained and improved in the future.

The same goes for risk exposure and risk tolerance. If the risk exposure is at or above the risk tolerance, the board of directors can have a serious discussion with management about how to limit the risks to an acceptable level. There is a balance between risks and rewards ... and if the defined risk tolerance is nowhere nearly utilized, the discussion could be on increasing the level of ambition and request that management becomes more aggressive and pursue even higher targets. Hence, the discussion of risks and risk exposure is not just one of restrictions and holding back.

Here are two generic examples of the benefits of having a defined risk tolerance:

- Company “A” wishes to expand into a new market, but the project involves significant risks (and has potentially significant benefits). Management discusses whether they should “dare” to pursue the target.

If the potential risks of the project, when added to the ERM portfolio, still holds well within the defined risk tolerance, then the decision is probably a sound decision. Management can have discussions of how aggressive (costs and investments) they can allow themselves to be in the pursuit of the new target.

If, on the other hand, the project makes the company exceed their risk tolerance, the decision on the new venture is prudently “no”.

- Company “B” has suffered a severe loss, and hence the approved risk tolerance in absolute value is reduced. This invokes that the company’s risk exposure exceeds the risk tolerance. Management needs to discuss measures to mitigate the risks, and possibly stop strategic development, which entails high levels of risk to comply with the risk tolerance defined by the board of directors. Management and the board of directors will need to discuss and re-define targets to a less ambitious level as the maneuverability of the company is reduced.

Comparing the risk exposure to a defined risk tolerance is providing a base from which strategic decisions can be made – prudently – and the explicit mitigation of risks becomes a strategic leverage/tool for the company.

## Closing Comments

In simple terms:

- a defined risk tolerance is needed to be able to address the risk exposure
- a risk tolerance can be defined based on the risk map alone
- you can [only] consolidate a risk portfolio by use of Monte Carlo simulation
- a consolidated exposure enables a portfolio based risk tolerance
- the risk tolerance can be used to discuss both whether the company is too exposed to risks or not exposed (ambitious) enough

The resulting reporting and discussions must be kept intuitively acceptable to management as well as to a board of directors, none of which are presumably risk management professionals. This is where strategic risk management becomes a competitive advantage, and the risk management community becomes value adding for the company.

For further discussion, questions and comments, please do not hesitate to reach out to me.

Hans Læssøe

**AKTUS**

[hl@aktus.dk](mailto:hl@aktus.dk)