The COSO organisation has recently published a guidance on risk appetite as a critical tool for achieving success.

https://www.coso.org/Documents/COSO-Guidance-Risk-Appetite-Critical-to-Success.pdf

This is not about the guide as such. I have a serious issue related to the term definitions themselves. According to the COSO guide:

- Risk **appetite** is the amount of risk you are **prepared** to take to meet your aspirations
- Risk **tolerance** is the amount of risk you are **willing** to take to meet your aspirations

What REALLY bugs me, is that this definition is exactly opposite to the vocabulary of ISO which in 2009 issues the Guide 73 where:

- Risk **tolerance** is the amount of risk you are **prepared** to take to meet your aspirations
- Risk **appetite** is the amount of risk you are **willing** to take to meet your aspirations

George Bernhard Shaw has been quoted to state that *"The English and Americas are two fine people, separated by a shared language"*. It appears the drive to increase confusion has not stopped yet. Personally, having English as my second language, I mentally like the ISO vocabulary better than the COSO – but I can easily live with either. So:

Dear ISO and COSO organisations. Get together and agree on terminology

COSO and ISO are both powerful organisations, and in a global business world we cannot avoid having risk managers using COSO meeting others using ISO – and hence destined to be misunderstanding each other when talking about e.g. risk appetite.

This is damaging for the "brand" or risk management and will be confusing to non-risk professionals who get in contact with the terminology on an occasional basis.

Usefulness of the concept

The usefulness of risk appetite and risk tolerance is often debated among risk professionals and thought leaders. Opinions differ greatly on a scale of being "pivotal for strategy design and business success" to "a compliance instrument" to "utter nonsense/waste".

Companies financial services and probably also other industries will find that some elements of risk appetite are defined by regulators. Other will find risk taking limitations are set by lenders, banks or other external bodies. When that is the case, adhering to the concept becomes a compliance issue – beyond focused risk management.

For others, and in other contexts, risk taking limitations are set by the Board of Directors and/or management and are more internal – yet expected to be observed.

My perception is, when done "right", the concepts of risk appetite and risk tolerance are tools which can guide decision making on operational as well as tactical and strategic levels.

In the remainder of this article, I will use the ISO vocabulary whereby:

- Risk appetite is the level of risk we are willing to take.

  This means that organisations should not seek to, nor use resources on managing risks when the exposure is below the appetite level. As a matter of fact, using resources on this is reducing competitive advantage and hence putting the company at more risk, not less.

  And yes. I have seen examples of companies that drove elaborate efforts to further reduce the potential impact of a risk exposure, they also deemed was well below their risk appetite. This most often happens when human biases “kick in” and the perceived exposure is bigger than the real one.

- Risk tolerance is the level of how much risk we are prepared, if need be, to take in pursuit of our objectives.

  This means that risk taking exceeding the risk tolerance is “unacceptable” either by external (regulator, bank) or internal (management) decision. Hence, risk mitigation is “mandatory” to reduce the exposure to an acceptable level.

  Few companies I know of, use risk tolerance to “boldly go, where no man has gone before” to quote the Star Trek. This depletes company development, potentially based on executive “fear”.

It follows from this, that risk exposures which are lower than the risk tolerance and higher than the risk appetite should be mitigated/addressed to the extent this makes sense from a general business perspective, and not as an element of risk management.

As the risk tolerance becomes the upper limit of how much risk you may take, I will, in the below, focus on risk tolerance and implicitly assume risk appetite is used in parallel.

Multiple risk tolerance statements

Some of those who advocate risk tolerance is useless, mention, that you cannot create one single statement, which will guide your decision making. This is true. The risk tolerance of any organisation will differ between categories/types of risks:

- You may have a very high tolerance for liquidity risks as you are well financed. This allows you to pursue bold endeavours.

- You may have a very low tolerance for health and safety risks as you do take good care of your employees.

- You may have a high tolerance for reputational risk as you are a commodity provided with an inconsequential brand name.

- You may have a very low tolerance for environmental risks as you do wish to be a good and responsible citizen wherever you operate.

Risk tolerance is, and must be, linked to your performance indicators/metrics, hence you will end up having a risk tolerance statement for each such metric. This means that some initiatives will be

limited by e.g. the safety tolerance whereas others will be limited by financial risks. That is life – no decision or endeavour is one-dimensional and linked to only one metric.

Furthermore, there will be one level of risk tolerance on executive/strategic level or subject to approval by the Board of Directors and another level used for individual decisions and/or projects.

Intuitively one may think the acceptable risk exposure, i.e. risk tolerance, on executive level is significantly higher than that of a single decision/project. Whereas this is true in absolute numbers where the C-Suite may be allowed to "lose" millions, this is often not true in relative terms as a project may accept a 100% loss on a known risky/exploratory endeavour. Especially the pharmaceutical industry is known to spend significant funds on projects/product developments which never become actual products.

Irrespective of whether on corporate/strategic level or on operational/decision/project level, it is valuable to operate with a risk tolerance. In a personal comparison, it resembles adhering to a defined speed limit, which is not defined to bother us drivers, but to ensure a reasonable level of traffic safety.

By the end of the day, there is no such thing as absolute certainty when addressing the future. As such, decision making and risk management is not about risk avoidance, but about intelligent risk taking. As stated by racing icon Mario Andretti "If everything is under control, you are moving too slow". The risk tolerance is deliberately deciding how fast you are or will allow yourself to go.

Facts, please

The above risk tolerance statements are useless as they refer to "very low" and "high". What does "very high" mean, and how low is "low".

In general, qualitative risk management is useless and only serve to add a false sense of security. Using qualitative measures will add human biases to the equation and makes the outcome of person A differ from that of person B and hence nullifies the value.

Risk management must be based on facts and data to add value to decision making.

Furthermore, the potential impact of any and all risks, opportunities and uncertainties must be measured in terms of the performance metrics used by the company. To be blunt. If you cannot measure the impact of a particular risk in any of the performance metrics you use to run the company, that risk does not affect company performance, and hence it is inconsequential, i.e. not a risk at all.

For each risk, opportunity and decision uncertainty you must define the outcome range as a statistical distribution, and for risks and opportunities, the likelihood this will materialize in the first place.

There will be multiple risks, opportunities and uncertainties in every decision. To calculate the combined exposure, you need to use Monte Carlo simulation as formula-based calculation is not a plausible approach. Doing that will enable you to monitor and report on outcome ranges and risk exposures as you will need.

Based on this approach, the above, corporate level, risk tolerance statements may be reworded to something like:

- The company may accept liquidity risk, when the 5% worst case negative liquidity exposure does not exceed 100 mUSD.
- Employee safety must be secured to the extent there is less than 1% likelihood of any permanent injury beyond 5% disability and less than 10% likelihood of hospitalization beyond 3 months.
- The company does not monitor nor measure brand and/or reputation.
- Management must ascertain environmental damages are contained within company premises. The likelihood of external environmental damage must be below 5% and the related clean-up costs must not exceed 10%mUSD any given year.

Effective risk management deals with upsides as well as downsides, and as such the company may also operate with positive risk tolerances:

- To ensure and focus on sustainable development, the company will not actively pursue growth beyond 20%. In effect this means if/when more than 20% growth happens it is driven by outside factors and potentially rare.
- The company will not pursue profitability exceeding 20% Return on Sales as this is expected to negatively impact brand perception. Again, higher profitability may occur based on externally events/circumstances.

Such statements will, along with a monitoring of current exposure, provide management with guidance on new decisions. From time to time, risk tolerances will hamper pursuit of some specific initiative, but I have also worked with companies, where the actual/current exposure was significantly below what was allowed by the Board of Directors. In essence, management were “driving too slow” and thereby not developing the company to the extent they could have done. That deprives shareholders value creation.

Risk tolerance, and hence risk appetite, can be a highly valuable management guidance tool.

Decision level risk tolerance

For individual decisions and implementation initiatives/projects, risk tolerance statements may be in line of:

- Project management must ensure a minimum of 40% likelihood of meeting the defined target, and must ensure a 95% certainty of providing a positive net present value.
- Project management must ensure at minimum 75% certainty the project is finalised with target date.

All of these statements are easily modelled and simulated using Monte Carlo simulation, which also in the so-called Tornado diagrams provide priorities as to which issues are most impacting the outcome should a plan not be in line with the defined project risk tolerance.

Hence, also on decision/project as well as on operational level will a defined risk tolerance and risk appetite guide managers to make better decisions.

Closing comments

My first and foremost request is:

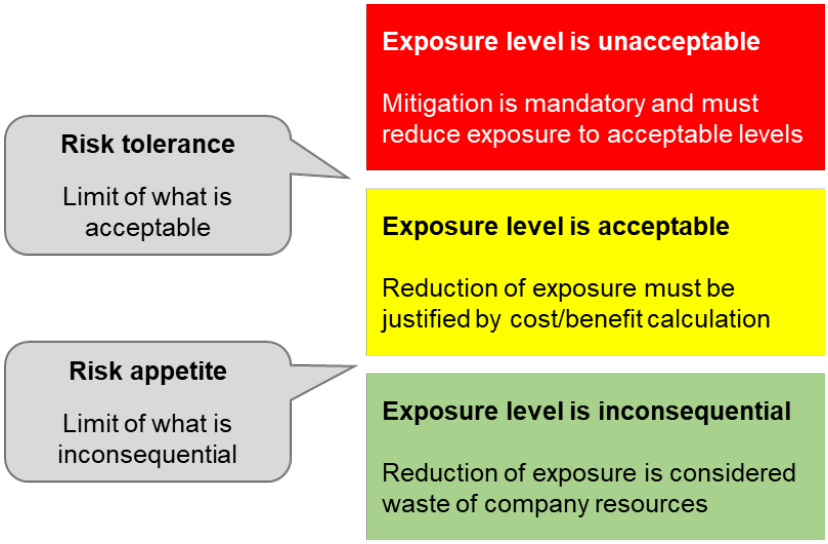
ISO and COSO organisations. Agree on terminology.

It is confusing to the world both within and outside the risk management profession to have two such powerful organisations deliberately contradict each other on terminology.

Secondly, the concepts of risk tolerance and risk appetite are very useful guides for decision making from company strategy to individual decision.

Cut short, two "boundaries" are defined and hence there are three levels of management of risks.

When based on facts and data and used as elements of quantitative risk management, risk appetite and risk tolerance are powerful tools of intelligent risk taking.



Hans Læssøe