The approach to and value of an Enterprise Risk Management (ERM) and the underlying risk register is widely discussed among risk practitioners. Schools of thought ranges from this being an essential methodology for governance and overview to considering the whole ERM being utterly useless and nonsense.

My view is somewhere in the middle of this as …

- I do not believe an ERM approach based on risk registers truly helps executives making the decisions they face or decide to make.
- I do believe, that applied effectively, an ERM approach is valuable and can drive decision making (which otherwise would not have been considered).

I believe the balance is struck by adapting some form of risk register and an ERM approach as a tool for the risk manager, and hence, not for the C-suite. This potentially simplifies the process of updating the ERM.

WHY ERM

One may validly contest, that as an ERM approach does not help managers/executives to make better decisions, any effort spent making it, is a waste of corporate resources and hence depleting competitiveness … and should be terminated sooner rather than later.

However, any organisation takes a vast number of risks and pursue a number of opportunities in parallel. Hence, if someone, the CFO, the CEO or the Board, wishes to have an overview of the potential exposure of the company – an explicit effort to create this is needed. It could be done by adding uncertainty spans and explicit risks and opportunities to the annual budget process – but this limits the risk metrics to purely financial metrics – and a company may (and probably should) wish to manage their risk taking on non-financial parameters as well.

Based on this, some process is needed, and ideally it should:

- Be as simple/effortless as possible … quoting Albert Einstein *"Simplify as much as you can, and no further".*
- Be holistic in risk identification on all parameters which the company wishes to address, be it financial, environmental, reputational, or employee motivation & satisfaction … or any other the company finds sufficiently relevant.
- Enable qualitative and quantitative assessments to be combined and used in parallel.
- Be precise enough to drive decisions … and no further.

The purpose of the holistic ERM program is providing the risk manager with a tool based on which he/she can drive decision making in the company – and hence lead to strengthening sustainable performance.

What I wish to cover is the situation where company A has a risk tolerance for liquidity of say 300. The normal operation uses a level of liquidity which fluctuates between, say 100 and 150 – well within the tolerance. On top of this, there is an identified risk of losing a key customer which will strain liquidity with additional 50. The project costs of two major projects within the company further strains the liquidity by 50 making the total strain up to 250.

Now the company is considering initiating a new project, which may strain the liquidity by some 40-70. Now the risk exposure is exceeding the 300 tolerance, and management needs to have this insight to make a good decision of declining/postponing the project, enabling further liquidity or sequencing some expenditures to stay below the tolerance level.

The good ERM approach spots the exposure of the risk portfolio … and enables/drives needed decision making in time.

HOW ERM

Based on the above purpose and value criteria, it is evident, that the ERM process is a tool for and driven by the risk manager and hence not an executive reporting tool. Deployment comes in a number of steps:

1. Define the performance parameters (financial, reputational …) on which the company wishes to manage their exposure.

   I suggest the risk manager, supported/challenged by relevant colleagues comes up with a limited set of parameters, including the rationale for choosing these … as well as the rationale for not choosing others that were contemplated.

   Then, the risk manager presents this to the executives for approval.

2. Define the risk tolerance for each parameter … simply asking the executives "*What level of exposure (balancing impact and likelihood) has to be, before you want to hear about it, and take action on it*". The risk is of course, that the CFO responds "*I want to know everything*".

   Again, I suggest the risk manager presents suggested/recommended levels for approval rather than having executives think from a blank piece of paper. This reduces the workload on the executives and provides the risk manager with a better possibility of getting tolerance definitions which are easy to work with.

   Note. This includes the element of time. Which timeframe is to be applied (e.g. coming year, this business plan period, …). The more agile the company is, the shorter horizon can be applied. If you can significantly change the company in 12 months, there is no need for looking at a three-year horizon. If your company is using long-term assets/investments and cannot change much within a five-year horizon, looking at a three-year horizon does not help/make sense.

3. The risk manager establishes/defines the risk register she/he will need to report to executives if/when needed – and collects the risk portfolio.

   Team up with company specialists from throughout the organisation. These people will rarely have a political (hidden) agenda but will raise real concerns and valid opportunities. Based on their insights, they will also be able to be quite specific in their descriptions. Lastly, and especially if coached well, they will have/know of data which enable at least semi-qualitative assessments, which are vastly more valid than even the best quantitative.

   I recommend using plenary identification brainstorms as people inspire each other.

Very importantly, the risk manager also needs to reach out to project managers/drivers in charge of major project and strategy implementation to include their risk exposure to be holistic.

4. The risk manager compiles the data in the tailored and "as simple as possible" risk register.

   Assessments for each risk are entered as, or of need be transferred into, figures based on the parameters chosen in the above step 2. Hence, any one risk may have multiple impact outcomes, but generally only one level of likelihood.

   As impact and likelihood are interconnected, I recommend defining and describing the impact first, and based on this (impact scenario) define the likelihood of occurrence.

   These assessments need not be more precise than what is needed for decision making. If an impact of 20 or 30 will lead to the same decision and action – there is little value in being more precise. I have found this applies to likelihood in particular and ended using the five levels of 1%, 3%, 10%, 30% and 67%.

   The risk manager ensures this is updated using a combination of two approaches:

   - Each risk is assessed for volatility, and an update frequency is defined. Some risks, like e.g. currency exposure in many companies, jump "all over the place" and need to be updated on a rather frequent basis to be relevant. Other risks, like a building fire, is rather static as a risk, and update can be made on a two or three-year basis without jeopardising data validity.

     Naturally – in between, things may happen that drives immediate updates.

   - When major new initiatives are taken, these are to be included in the risk register … and when initiatives are deployed/finished, they can be taken out.

5. Monte Carlo simulation is applied to consolidate the exposure on each parameter to "calculate" the overall exposure.

   When modelling the impact parameters, it is important to cater for human biases, and apply adequate ranges around the assessments. I have often used a very simple triangular distribution based on a factor of two. If a risk was assessed to have an impact of 300, then I used 300 as most likely outcome, but used 150 as minimum and 600 as maximum. This is by no means perfectly valid math, but in my experience, it is precise enough to drive decisions and the distribution is easily explained to people without a mathematical background.

   The simulation outcome is then compared to the defined risk tolerance, and the risk manager decides whether or not there is reason for executive reporting.

6. Executives and boards receives tons of reports, and it is not valuable to the management of a risk portfolio to receive monthly, quarterly or other systematic reporting which generally states "no changes, all is well".

   Risk reporting should be exception based only. That is, if/when something happens, which leads to either one of the tolerance levels may be exceed – the risk manager addresses and verifies the data, and report on whatever has happened to make this risk tolerance to be exceeded. If management has a reporting template (some do) – use it.

Ideally, and in collaboration with relevant specialists, the risk manager pinpoints key drivers (leveraging the Monte Carlo Tornado diagram) and recommends one or more actions to be taken to bring risk exposure below the risk tolerance as part of the reporting.

To the extent needed by legal or other requirements, the risk manager can, and should be able to use the risk register to "auto" generate any standard reporting needed.

ERM VALUE

This approach has, I believe a number of valuable properties.

- It is as simple as possible for the organisation.
- It is systematic and holistic.
- It does not involve executives more than needed and is designed to support these in their decision making and execution.
- It allows intelligent risk taking.
- It positions the risk manager as a person to be listened to – and who speaks up when needed.

This way, the ERM database becomes the tool for the risk manager, just as the General Ledger is the tool for the financial controller rather than for the CFO.

CLOSING

Any company applies a multitude of risk management approaches in parallel. The treasury function is using a currency hedging program to cover for the risks of foreign trade, Purchasing is addressing vendor delivery risks as well as hedging commodity prices, IT is ensuring IT security and backups, the risk function ensures an effective insurance program is in place, etc., Legal is driving legal compliance, including scouting for and addressing competitor infringement, etc.

Furthermore, proactive companies are systematically embedding risk and opportunity considerations and analytics in decision making when deciding on projects or initiatives.

All of this is "case by case" or looking at one issue at a time.

Some companies will have an ERM approach – and using the above approach, this can be a valuable tool for the risk manager to drive executive decision making when needed to ensure risk taking is in line with the defined risk tolerance.

Without this holistic ERM approach, the company may unknowingly take unacceptable risks, or, as seen more often, not even remotely utilize the risk tolerance they have, and hence move too slowly. Quoting racing icon Mario Andretti "*If everything is under control, you are moving too slow*".

Hans Læssøe
AKTUS
hl@aktus.dk
www.aktus.dk