These days, risk management is a rapidly evolving discipline, where new approaches add to traditional risk management in parallel with the traditional being increasingly professionalized and advanced. In this context, the risk management profession experiences significant changes in tasks, responsibilities and organisational positioning.

To a risk manager, this is not a bad development, rather an avenue of growth and enhancement. However, it does add to the skills required and methodologies applied.

The purpose of this paper is to provide inspiration on how to go about this – growing from a Traditional risk manager to be an Enterprise and potentially a Strategic risk manager. Please note, that this sequencing is not a description of an advancement, rather than a change. One element of risk management is not more sophisticated or more important or valuable than any other.

The paper will have four sections:

1. Categories of risks and their handling differences
2. The role and responsibilities of the Strategic Risk Manager
3. Ways and means to become a successful Strategic Risk Manager
4. Further development into proactive Strategic Risk Management

The intention of this paper is to serve as an inspiration. Strategic Risk Management (SRM) is still so new and changing/evolving that there is no one fixed formula. The ISO 31.000 standard of risk management has it as a guiding principle that risk management must be tailored to the organisation, and hence recognizes that there is no “one size fits all” or even “industry best practice” approach in existence.

In this paper, the term organisation is deliberately applied. This paper should be valid for corporate entities as well as not-for-profit and public organisations. The goals and aspirations of these different types of organisations differ, and hence their definition of “success” – and their risk management focus.

However, the processes and approaches to manage risks will be largely the same irrespective of organisational type. A business entity and a non-profit organisation operating in multiple countries both face currency volatility – and will have the same inclination to deal with this – more depending on the magnitude of exposure than on type of organisation.

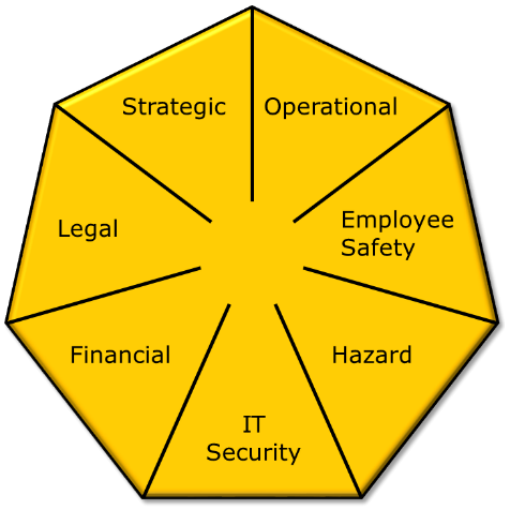
1. Categories of risks and their handling differences

Risk management as a professional discipline is not new, and industries have identified, assessed and addressed multiple risks for more than a century. Most common are mitigations such as insurance programs, where the exposure to a risk is transferred at a premium to a vendor capable of absorbing the financial loss. Hedging of currencies and other financial instruments also serve to protect the value of a company/organisation.

As the risk management industry has evolved, more risks are addressed, as indicated by the “umbrella” shown here.

Many companies and other organisations have processes and organisational entities in place to cater for most of these types of risks, be it…

- Operational risks
- Employee Safety risks
- Hazards
- IT Security risks
- Financial risks
- Legal risks
- Strategic risks



Common for these is largely, that the appointed risk manager "owns" the risk portfolio and is the one defining and ensuring execution of the management of these risks. The exception in point for many industrial organisations is the "operational risks" which are more or less explicitly embedded in the day-to-day running of operations.

Based on this, the risk manager needs experience and expertise in identifying, assessing, prioritizing and handling risks, whereby the rest of the organisation rely on the risk manager to be "in control". A few examples:

- The head of the Insurance function defines and purchases the insurance programs needed to comply with the guidelines from Board and Management. That is, guidelines he has often been championing preparing/defining for management and Board approval
- The head of Treasury defines and hedges the currencies needed to the extent matching the provided guidelines
- The head of IT Security defines the measures to be taken so safeguard the organisations use of IT. Originally, this was very focused on back-up routines. Whereas it has evolved into access protection, data protection and protection against different types of cyber-crime – which currently is a "fast growing industry"
- The head of Legal defines the controls needed to ensure "proper" behaviour from the organisations employees (at all levels) and executes on these through training and auditing. Note, that the head of Legal Affairs may not be seen as managing risks, or see that as a focus area – despite the efforts to guide and control behaviour.

Hence, the risk manager needs strong professional skills within his area, as well as capabilities to operate with the Board and Management of the organisation to get the mandate to do the job well. The more professional and qualified the risk manager becomes, the more trust is put upon her/him, and the better (s)he will be able to perform.

In this paper, the above elements of risk management are noted as traditional risk management. As stated, this is not to belittle the efforts, professionalism and value of these elements of risk management – just to group these based on the characteristics of these in relation to the risk manager role.

All of this is, as stated, in place in most mature companies. Over these past few decades, more and more organisations have included Enterprise Risk Management (ERM).

In its nature, ERM does not add to the risk portfolio but is mostly an explicit approach to ensure optimal alignment across the types of risks handled in silos throughout the company. Hence, the value of ERM is to ensure a systematic overview of the risks faced by the organisation as well as an alignment to ensure that e.g. operational risks are not "left to chance" whereas asset risks are insured to the very last penny.

ERM builds on the notion that no chain is stronger than its weakest link – and hence, that strengthening the already stronger links does not reduce the overall exposure of the organisation.

This also entails that the role of the Enterprise Risk Manager is more coordinating, aligning and cross company collaborative than that of the traditional subject matter focused risk manager. It is often the task of the Enterprise Risk Manager to develop and provide a coherent reporting to Board and Management on overall risk exposure than directly being involved with managing explicit risks.

This leads to a new set of skills needed to be successful as an Enterprise Risk Manager. These are elements such as:

- Business/Industry understanding and overview
- Broad (rather than deep) risk management acumen
- Collaborative and communicative skills

In many organisations, the role of Enterprise Risk Manager is held by one of the people handling an element of the traditional risk management, e.g. being the head of insurance. However, it should be noted, that in the role of Enterprise Risk Manager, tasks and approaches are quite different from those of the traditional risk manager.

Very few organisations appoint a head of Enterprise Risk Management who then becomes head of all initiatives related to risk management throughout the organisation. Even in companies that have an explicit Chief Risk Officer position, it is rare that this CRO has more than directional responsibilities as to risk management across the company.

The gradual evolvement of ERM found that the element of identifying, assessing and addressing strategic risks (SRM) emerged as a natural element added to the "umbrella" above.

Beyond the risks already catered for, the risks related to the strategic positioning and/or direction of the company were not risk managed systematically. That said, most organisations had some processes and controls to address such risks and were making analyses to identify and assess some strategic or business risks. The missing link was the systematic approach.

There are two types of strategic risks to an organisation …

- The current, i.e. the risks emerging from the organisation being as it is, doing what it does in the environment in which it does this. These may be competitive, legislative, market, technological or like risks

- The future, i.e. the risks emerging from the strategic direction and explicit strategies and goals the organisation pursue

Inherently embedded in these, and largely not addressed as part of traditional risk management, the strategic risks and risk taking also entails a level of reward, i.e. opportunities.

These differences mean that strategic risks differ from the traditional in a number of ways:

- There are opportunities to identify, assess and potentially pursue as well as risks to address. This is as much or more about creating- than protecting value
- Strategic risks tend to be opaque to a significantly higher extent that traditional (just as strategies are less tangible than plans). Hence opacity is the name of the game
- They may emerge from outside the organisation as well as, but to a lesser extent, from within the organisation and hence, identification starts outside the organisation
- The strategic risk manager can never "own" the risk, as he will then get to own the strategy and eventually (in the CRO role) becomes the head of everything in the organisation

Strategic risks as such are hence VERY different in nature, and call for a different approach of handling. That said, the key elements of risk management still apply – the approach of deploying these just differ.

Based on this, the successful strategic risk manager needs a very different set of skills:

- A very strong business acumen and communication capability
- Ability to holistically see impact across the organisation
- Very strong collaborative and coaching skills

On the other hand, strong professional risk management skills are less needed. Not that they are not needed, but prioritizing between hard core risk management skills and business acumen, the latter is most important for a strategic risk manager. As such – moving from Traditional to Enterprise, and then to Strategic Risk Management is a significant change of position, task and working day. Note that whereas the position is different, it is not necessarily a promotional change.

2 The role and responsibilities of the Strategic Risk Manager

As a newly appointed Strategic Risk Manager, the organisation may start to rely on you to handle the strategic risks of the organisation, and hence relieving management from that task. It is paramount to your success that you make sure everyone understands that being a Strategic Risk Manager does NOT mean that you own and mitigate strategic risks.

An example of my own. At a point in time, I was giving a presentation to the leadership of Procurement about what I did and what I was trying to accomplish for the organisation. After that and a few questions, our head of procurement stated, *"so, Hans is in charge of managing our strategic risks, and it is great that we now have this role in the company"*. I saw that I had not communicated my role well enough, and decided to take him up on this. I said*: "Yes, looking at Procurement, our biggest risk is related to*

demand volatility – so to mitigate this risk I would like you to ensure that we only use vendors that can deliver on-site within 48 hours. I recognize this will hamper our use of Asian vendors, but we really cannot wait having goods in transit for 6-8 weeks".

As expected/planned, this took the head of procurement somewhat by surprise, as the company does use a range of Asian vendors, and he stated *"That is, fortunately, not your decision to make"* – which I agreed upon and responded: *"Correct, the risks related to procurement are yours to handle. My role is to ensure that you deploy an explicit and systematic approach to identify, assess, prioritize and mitigate them – not to tell you how to run your business. I am certain you do that better than I could"*

Hence, the role of the Strategic Risk Manager is not to define how to mitigate risks or pursue opportunities – but may very well be as a knowledgeable sparring partner in the task.

The responsibilities of a Strategic Risk Manager are mostly to:

- Provide a coherent framework in which to identify, assess, prioritize and treat strategic risks and opportunities. This framework includes elements such as:
    - Overall frames and risk tolerances
    - Methodologies and training
    - Tools and templates
    - Reporting means
- Drive the deployment of this framework for current as well as future and emerging strategic risks through close collaboration with middle and top management throughout the organisation
- Act as "point of contact" if/when things happen in the surroundings that may impact the organisation and which have not already been catered for, e.g. handling a Brexit (The UK leaving the EU), if this has not been addressed already prior to the UK Referendum
- Enable that the reporting and handling of strategic risks are seamlessly embedded in ERM (as this otherwise would lose credibility)

The head of ERM will, in many organisations, also have the role as head of Strategic Risk Management as both are overview and collaboration based more than deep professional skill based positions.

If a traditional risk manager wishes to transfer his career into ERM or SRM, he must be highly aware of the change of working day, change of role and focus – away from risk management, and into "business" management irrespective of what the business of the organisation may be.

3 Ways and means to become a successful strategic risk manager

To the layman, risk management is risk management and the real change of role, responsibilities and tasks of moving from a strong professional traditional risk manager to become a Strategic Risk manager may not be very clear. However, pursuing this, it is important to both know and consider the changes. Otherwise you may end up in a position that was not as inspiring and good as you thought it would be.

There are a number of skills you need to attain to be able to do the job. That said, you may not need or have all of them from day 1, but you will need a planned way to get them.

Business acumen. To be able to talk to, and inspire, organisational leaders to identify and manage their strategic risks, you must be able to talk to them on their terms, including understand their part of the "business" the organisation is doing, their goals and aspirations and their measures of success.

You must also be able to see their area in the context of the whole organisation as well as to the environment in which the organisation works. You need to have access to or knowledge about what happens in the environment in order to support the leaders in managing emerging and external risk … as well as pursue external opportunities that will arise, and can be developed by deliberate actions on behalf of the organisation.

Value Creation Mindset. The role of a Strategic Risk Manager is as much about creating value to the organisations as it is about protecting value. Any pursuit of a potential opportunity is creating value, whereas mitigation of a risk that is already existing is more about protecting value.

The distinction is mostly academic and if you are uncertain whether this particular action is value protecting or creating, it is not that important.

Coaching/asking role. You are no longer the owner of the risks you address – and it is paramount that you do not allow leaders to "brush off" the risk to you. As a traditional risk manager, or in many other positions you may have had prior to becoming a Strategic Risk Manager, your job/task has perhaps been to be the provider of answers. Mine certainly was prior to becoming a Strategic Risk Manager. This is over.

As a Strategic Risk Manager, you provide the framework, i.e. tools and processes to manage strategic risks, you do NOT do the management of the risks or define the actions to be taken. Hence, an effective approach is to refrain from responding to questions beyond those related to the use of the framework, but rather ask and coach leaders to define which risks they see, how serious the risks are and what they intend to do about them.

As you grown in the role, your asking style will become stronger and leading questions are OK if/when you need to direct a leader to see a specific topic he has not thought about on his own. You will also learn to ask different style questions to different leaders as some wishes to be challenged whereas others will see any challenge as a (personal) attack on their professionalism (and throw you out of the office). Furthermore, you will learn things from leader A, which will inspire you to discuss further with leader B.

Proactivity. A lot of traditional risk management is about safeguarding and protecting value of the organisation. Strategic risks are as much about being proactive and hence drive risk taking. The purpose is not to avoid or minimize risks, but to take calculated risks, and do it well. One organisation expressed the purpose of their strategic risk management as *"We make money by taking risks, but we lose money, if we do not manage the risks, we are taking"*. This captures the nature of strategic risks well.

This also means that when you have gained sufficient trust amongst management, you may get to a position where you actively recommend that the organisation take on more risks to pursue higher goals, or to meet goals, which appear to be in jeopardy. The purpose of risk management, especially strategic risk management, is not to avoid risks, but to provide Board and

Management with a reasonable assurance that the defined goals can be met with the initiatives taken cf. The COSO definition of the purpose of risk management.

Beyond these explicit skills, you will need to have a framework within which to operate. The organisation you work for may already have defined and deployed this. However, as Strategic Risk Management is still not widely applied, you may very well be in a position, where you need to develop an SRM framework.

The below is based on the RIMS Strategic Risk Management Implementation Guide, but are edited extracts to let you know how to execute the role of Strategic Risk Manager. Hence, none of the below is actually new – but is applied in a different setting which affects processes, data etc.

In a somewhat prioritized order of sequence, this framework should include the below elements.

Identification. Which processes do you put in place to identify the strategic risks of the organisation? You may very well interview top managers as well as (highly recommended) senior specialists what they see as potential risks for the organisation. You may also (possibly in a phase II) look for external sources or sources looking at the external world for risks to the organisation.

Phase I. Start focusing on the risks that the organisation expects you to look at. The systematic search for and inclusion of opportunities is more likely a phase II or III in your development of SRM.

You will also need some form of database or the like to collect the risks. Many new SRM heads start with a simple spreadsheet – but depending on the size and complexity of the organisation, this may become inadequate within a brief period.

In the identification, it is important that you do not dismiss any risks. As risks will be subsequently assessed, early dismissal may lead to eliminating a severe risk.

Assessment. You have to define and apply a consistent approach to assessing the individual risks to enable a prioritization between these. This has to be detailed enough to enable adequate prioritization, yet as simple as possible to ease the deployment and use by the non-risk-managers who own and have to assess the risks in the end.

A High/Medium/Low grading is often used, but will soon be seen as too coarse to deal with the more extreme risks you will encounter. Hence a 5x5 (i.e. Very Low … Very High) is recommended. Further detailing will often add more complexity than value. However, this is where the risk management needs to be tailored to the organisation.

The assessment scales will need to be specific and explicitly defined so that everyone involved knows what differentiates “High” from “Medium”. Logarithmic based scales are common where e.g. “Low” is twice the level of “Very Low”, “Medium” is twice that of

Risk Assessment scale examples

Rating	Likelihood	Financial	Reputational
Very High	90%	> 2.000	Global
High	30%	1.000-2.000	Regional
Medium	10%	500-1.000	National
Low	3%	250-500	Local
Very Low	1%	< 250	-

"Low" etc. This is due to our minds being logarithmic. We can distinguish between 1% and 3%, but without data, we cannot tell 40% from 30%. This goes for both the impact and likelihood scales.

On the impact scale, you may opt to use multiple scales depending on the organisations risk tolerance towards different impacts of risk. So, there may be one scale for financial losses, another for employee safety, a third for brand/reputation and a fourth for environmental risks. Note, that some of these scales may be defined in terms of verbal descriptions rather than numbers. As a Strategic Risk Manager, you need to ensure these scales are made and approved by the Board/Management.

You need, in your database, to be able to enter the assessments of the risk – both as the gross or inherent risk (i.e. the impact/likelihood given that you will not do anything in particular for this, beyond "normal business") and as net or residual risk (i.e. the impact given the effective deployment of the treatment defined).

Handling. You need to collect data as to what is being done to mitigate each risk. Data should include the "owner" i.e. as precisely as possible appoint who is responsible for taking this or that action to mitigate a risk as well as a description of the actions to take/taken, and as precisely as possible the effectiveness of these actions.

Descriptions of mitigating actions may link to defined and documented processes or other already available documentation. When ready, you may add elements such as the mitigations assumed effect on impact and/or likelihood of the risk as well as a measure of "quality" and timing.

When handlings are defined, you may find it relevant to liaise with Internal Audit to validate that mitigations defined are actually executed as described as the effectiveness is otherwise in jeopardy.

Mitigations should not include actions you consider taking or may/can take, but have not decided to take. The "could have"/"would have"/"should have" do not provide active mitigation. This is explicitly noted as such "wishful" mitigations are commonly seen in risk management registers.

Reporting. You need to have some level of reporting of the strategic risk portfolio. If you already have an Enterprise Risk Reporting in place, the strategic risks are to be folded into this in a coherent and consistent way. If not, you need to develop a new reporting, which may then grow into becoming the ERM reporting of the organisation.

The report should be as simple as possible and focusing on driving a discussion on the strategic risk management status as well as where to focus going forward with the Board and Management. The purpose should not be "documenting we are in control" as this will lead to a reduced attention to risk management which is potentially dangerous.

As a Phase II, the ERM/ SRM reporting should include some level of consolidation of the risk portfolio.

Gross Risk		Very Low (< 250)	Low (250-500)	Medium (500-1.000)	High (1.000-2.000)	Very High (> 2.000)	Grand Total
Very High	(90%)			1			1
High	(30%)		3	3	3	2	11
Medium	(10%)	5	7	11	8	3	34
Low	(3%)	3	6	9	14	5	37
Very Low	(1%)	1		2	2	3	8
Grand Total		**9**	**16**	**26**	**27**	**13**	**91**

This may, at first, be done using a simple heat-map (an example shown here, where the cells show the number of risks in each combination of impact/likelihood), whereas more advanced approaches can include a Monte Carlo based simulation of the risk portfolio and hence showing e.g. a 5% worst-case loss of profit/value/…

Furthermore, the reporting must highlight key risks to discuss. These need not always be the "top 10" as several of these risks may be rather static and not drive a discussion and inherently ignoring the less, but more dynamic risks.

The above is linked to the management of current strategic risks. Once this is in place, you may progress to more proactive strategic risk management and provide frameworks (tools and processes) to address the risks emerging from the development and deployment of strategies.

4 Further development to proactivity.

Developing, probably in a "Phase III", into a more proactive approach to manage strategic risks can further expand the influence and value of the Strategic Risk Manager. This is about how your organisation defines strategies and how do you identify, assess/prioritize the risks and opportunities emerging from these strategies – and how is this managed.

Once the strategies are defined – how do you deploy these, which risks and opportunities emerges from these initiatives … and how do you manage these risks.

However, as Strategic Risk Manager you must be aware that having the management of current strategic risks must be reasonably in place before management will let you direct your attention to the more proactive approaches.

Nevertheless, some ideas to use as potential inspiration.

Scenarios, where the Strategic Risk Manager challenges the team defining the strategy as to "what if" some of the key assumptions about the future proves not to be true, i.e. the world changes in a different way than what was planned/expected.

Amongst others, the RIMS Strategic Risk Management Implementation Guide provides more focus on how to implement strategic risk management in your organisation. Such scenario workshops have proven to be highly valuable.

The outcome of this process is essentially a prioritized list of "issues" which are to be handled in order to increase the success of the strategy. These issues may be opportunities (if the organisation choses to pursue these in time) or risks to handle.

Success based disruption, where the strategic risk manager leads a workshop among relevant people to discuss and address:

a. What are the key drivers of our success

b. What would it take to destroy this

c. How do we deal with these risks

This process may help participants spot even severe risks to the organisation e.g. imagine the Taxi industry had seen Uber coming 2 years before the first launch, or the music industry had seen iTunes.

Spotting such risks in time moves them from being "Black Swans" to being risks, the organisation can act upon and mitigate in time.

Disrupting Opportunities. Whereas the above success-based disruption is largely focused on identifying strategic risks to the organisation, this process is similarly focused on identifying strategic opportunities to the organisation.

20 years ago, it was stated that you must *"dominate or die",* i.e. if you did not have a dominating market share, you were doomed to follow the directions of those who were dominant, and you would eventually die. Today, it is more *"disrupt or die"* and hence, if you are not prepared to change and even disrupt the business you are in, then you will be forced to follow those who do – and play by the game rules of others … and die.

The process is similar to the above. Gather a team of relevant people and look at the environment you are operating in. Then ask – how can we change the "rules of the game" to something, where we have a significant advantage. There are three overall avenues of thought to deploy:

a. Price – e.g. What would it take to deliver (all/part of) what is delivered today at very little/no cost at all to the customer (e.g. online news)

b. Quality – e.g. What would it take to give the customer a superior quality perception in terms of product value, delivery speed convenience/ease (e.g. Amazon)

c. Community – e.g. What would it take to liaise closely with the customer in a dialogue of personalisation (e.g. Facebook)

Naturally, the most successful disruptors apply multiple avenues in which to disrupt and thereby create a new platform based on the game rules of the organisation.

These are mere examples of proactive risk taking/managing processes. In any instance, closely linking to the strategic planning process of the organisation provides the Strategic Risk Manager with an opportunity to leverage his expertise to drive discussions that eventually define robust strategies – and an easy approach to define, assess and handle the risks that remains being relevant to the organisation.

Closing Summary

The role of a Strategic Risk Manager is quite different from that of a Traditional Risk Manager, and even an Enterprise Risk Manager. The role is less specific and requires less of a deep professional expertise – but rather a broad and strong business acumen coupled with strong communication and collaboration skills based on coaching.

The Strategic Risk Manager can never own the risks he is managing, but rather has a role that may resemble that of the Finance/Budgeting function in an organisation. The budget team does not earn the money, nor do they spend the money – but they own the process, the database and the reporting on the financial performance, and they have the responsibility to raise management attention if/when things go astray. The same is true for the Strategic Risk Management function. They should own the process, the database and the reporting, but not the "content" (i.e. risk handling) but raise the attention of Management if things go astray - or better, before.

You need a framework, and if the position is new, you get to develop this as your first task. This will then evolve as the Strategic Risk Management of your organisation matures.

Finally, your position will move from being a problem solver (risk manager) to being a business partner to management.

There is support in the RIMS Strategic Risk Management Implementation Guide, other RIMS papers as well as the COSO II and ISO 31.000 standards to support your endeavour. However, be aware that these are generic bases – every organisation is unique and needs to define its own deployment.

Good luck

Hans Læssøe

AKTUS