Is Risk Management redundant?

Transcript of the presentation by Marinus de Pooter at the Risk-!n Conference in Zurich on May 19, 2022. He challenged current risk management practices and shared recent insights in dealing with the uncertain future.

These insights have major ramifications for risk managers, compliance officers, privacy specialists, information security officers, safety consultants, business continuity experts, resilience people and internal auditors. To name a few categories of professionals who love to talk about risks all the time.

To them managing risks is part of doing business as much as fireworks belong to New Year's Eye. And many people find doing a risk analysis just as self-evident as preparing a budget. However, it is not without reason that the beyond budgeting movement has come up.

In this context 'redundant' means: unnecessary. So, the question is: Is risk management as a separate system or program or function superfluous? In other words: can a management team be successful without the paraphernalia of risk management?

Conventional risk management is a structured approach to deal with the uncertain future. Applied in many organizations it is aimed at identifying, analyzing, mitigating and monitoring all sorts of risks. The underlying idea is that there are loads of risks out there. And that you got to do something about them.

According to many risk management can and should be implemented. Or even they say that it is absolutely unwise not to do so. It saves you from unnecessary pitfalls. And above all, risk management helps you achieve your goals.

In risk management approaches typically people check what can go wrong in the future. They then make substantial lists of risks (risk portfolios, inventories, registers). Tim Leech and others call this "risk list management".

Great importance is attached to completeness. As a result those risk lists are not only long, but also wide: easily many columns in a spreadsheet. The risks are usually categorized using a taxonomy. And prioritized using risk scores, based on risk criteria for likelihood and effect with scales ranging e.g. from 1 to 5 or 6 or 10.

Control measures play an important role in this approach. According to the experts you absolutely need controls to mitigate your risks. By the way, when you hear that verb – to migrate – you can be sure that you are dealing with conventional risk management.

Finally, periodic reports with information on the "state of risk" are submitted to the management team or the Board. You'll recognize this from your own practice.

What would be the ramifications of redundant risk management?

Suppose - as a thought exercise - that risk management were indeed redundant. What would be the ramifications of this, for example for internal auditors? These are the people in business who are supposed to audit risk management.

Internal auditors love to talk about risk. You can hear them talking about "my risks" in an affectionate way. Auditors seem to believe that the rest of their auditwork is easypeasy once they have a good understanding of the applicable risks.

This has to do with the international standards for the practice of internal auditing. One of them (#2120) states that the Internal Audit function must evaluate the effectiveness of the risk management processes and contribute to improving them.

In COSO ERM 2004 Risk Management was still seen as a process. COSO ERM 2017 came up with a totally different definition: ERM is the culture, capabilities and practices that organizations rely on to manage risk in creating, preserving and realizing value.

Based on another standard (#2010) the Chief Audit Executive must perform a risk analysis at least once a year as the basis for the risk-based internal audit plan. All this is to provide sufficient assurance that the significant risks have been effectively mitigated by the risk management and control systems.

And the organization's audit universe must include all major risks: the so-called key risks. Apparently, the underlying idea is that organizations have to deal with risks. So, you might think: It can't be true that risk management is redundant.

There are quite a few people working in the risk management world. Such as those who have been appointed to "risk owner" by their Risk Management colleagues. Or people who are members of a Risk Committee.

Some people are even Chief Risk Officer – the supreme risk person in their organization. And I'm not even talking about the countless risk managers, risk consultants and risk management software suppliers. Not to mention all the individuals who are busy in their organization with finetuning risk appetite statements, Control Risk Self Assessments and risk dashboards.

But …. if risk management is the answer, what was the question again? How well does conventional risk management help decision-makers deal with uncertainties, disruptions and dilemmas? Or is it more like a belief system? Could there be missionaries, believers and inquisitors who have commercial interests in maintaining this entire system?

Let's have a look at the real world. Decision-makers are busy creating and protecting what their core stakeholders value. That, in practice, always involves competing or even conflicting interests.

Imagine that a commercial music festival is being organized in a town. A municipal permit is required for that. As far as the visitors are concerned, what they hear sounds like music to their ears. But loud music is very invasive and many local residents probably experience it as a load of horrendous noise.

You can pick any other situation involving competing interests. Then a decision has to be made about something that is at stake that people value. Decision-makers have multiple options: doing something or refraining from doing it.

Now suppose that the following applies to these decision-makers:

(1) They look ahead constantly as part of their daily management activities. They seriously ask the question: what-can-happen? And they analyze how events and trends could help or hinder the interests of their core stakeholders.
(2) They show that they are consequence conscious and try to make realistic estimates of possible both positive and negative effects. That is, they consider the potential impacts of their options on the competing interests. And they realize that when they choose an option because of the estimated benefits, they still have to deal with the associated downsides.

(3) They demonstrate that they have proper competences and intentions to weigh the estimated effects on the interests at stake. They appreciate unwelcome information. And they deal with dilemmas in an equitable, fair way.

The key question is: Do they need separate risk management? Or is this all about their ordinary management duties? Before we dig into this a bit deeper I invite you to have a brief look at the development of conventional risk management.

How did the current risk management practices come about?

As early as the 1960s the first requirements of the Securities and Exchange Commission emerged in the United States for the inclusion of risk factors in documents in the context of Initial Public Offerings. In 2005 there were requirements to include risk factors in annual and quarterly reports. This concerns factors that make a share speculative or risky for a shareholder.

This grew into the requirement to have a Risk Management Framework. This is generally understood to mean: a coherent set of risk identification, analysis, mitigation and monitoring. It was aimed at preventing financial losses for those involved. Who – apart from the fraudsters – doesn't want that?

In order to better understand the current practices of conventional risk management we need to have a look at the origin of the risk registers, too. The risk inventory lists became fashionable in factories in the 1970s. There they had started using lists with all kinds of points of interest regarding the safety of the workers.

When there came more and more regulation in this area those lists were used to draw attention to possible dangerous situations. These lists were soon given a function in the context of compliance: they were useful for the inspectors who came to check the companies' conformance.

Legislators and regulators subsequently embraced these standards as methods for demonstrating that organizations have their affairs in order. "Doing risk management" (read: keeping proper risk lists) was gradually seen as a characteristic of good organizational governance. However, those points of interest were never primarily designed to achieve balanced decision-making.

Nevertheless, it has resulted in the practice that periodic review of those lists is regarded positively in the context of compliance. Namely to show that the factory management has thought about how the safety of the employees could be endangered. And that they have taken appropriate measures to mitigate those risks. If you come across a list of risks, for example in project plans and risk reports you know where they come from.

In the financial sector legislators and regulators went one step further. There they came up with a Risk Management function that must be independent of management. That function must inform the Board based on its own risk assessments. That function has so to speak the role of the sheriff who must ensure that certain cowboys do not screw up things.

Having an independent separate Risk Management department implies that colleagues quickly think: If you have queries about risks, you should contact them, because they are the experts. You should especially ask yourself how realistic it is to assume that with a herd of risk and compliance officers one can keep the cowboys in question on the right track.

If line managers are only held accountable and rewarded for their commercial performance, compliance will soon be defeated. You probably also know people who reason like this: "If they don't want us to do this, then they should outlaw it." Or: "Fines from regulators are just ordinary business costs." Reconciling dilemmas is all about attitude and mentality.

Due to their role, supervisory authorities are hardly interested in the 'upside' of risk. Many directors see risk management primarily as a compliance matter. To them, effective risk management means above all that they don't get into trouble with their external or internal supervisors.

Many brochures and articles about risk management try to get away from the compliance angle. They argue that in rapidly changing times business men, like sailors, must skillfully navigate turbulent waters. They say that understanding and managing risks is absolutely necessary (in risk management brochures you'll read the term 'imperative') for successful leadership. It constitutes your business case for implementing risk management.

Internal specialists and external consultants used risk management practices to help organizations reduce their exposure to undesirable consequences. It led to all kinds of methodologies and codifications of best practices: the internal control and risk management standards. Board members are taught to ask about the top ten risks. That is apparently a sign that people have thought carefully about their vulnerabilities.

In the 2004 edition of the COSO ERM Framework risk management was seen as a process. If you hadn't set that up yet, the consulting firms were standing in line to help you with the implementation. With risk analyses, risk profiles, risk frameworks, risk appetite statements and risk reporting.

The more these best practices were made mandatory, the more lucrative the revenue models of the advisors became. Extensive maturity models resulted in more and more bells and whistles. Numerous dedicated ERM and GRC applications have been developed with ESG solutions as the latest product line. It's now a multi-billion dollar industry with significant commercial interests.

It is striking, however, that you very rarely encounter entrepreneurs, directors, line managers or project leaders at risk management conferences and training courses. That's quite surprising really, since risk management promises to help them achieve their objectives better. These people aren't retarded. If it would really help them, wouldn't they sit in the front rows and learn how to take advantage of the recommended practices?

Risk management has developed into an accountability instrument. Decision-makers are expected to demonstrate how well they are able to prevent and detect things that might go wrong. And that is quite different from an approach to achieve your goals under uncertainty. You'll recognize it from your own experience. To which extent do these practices actively help line and project managers to make better decisions?

What is particularly problematic about conventional risk management?

It all starts with the core concept of 'risk'. What are we actually talking about? Unfortunately, there is no universal definition of the term 'risk'. In common parlance it has multiple meanings:

- the chance of an (unwanted) event happening;
- the cause of that event, like a risk factor or risk driver;

- that event itself;
- the consequences of that event, also called impact, implication or effect.

It is salient that ISO – the international organization for standardization (mind you!) – uses more than 40 different definitions of risk in its own documents. By the way, something similar also applies to "in control". Many initiatives are started to arrive at "in control statements" – without carefully checking first what the hack do we mean by "in control".

So the term 'risk' itself is pretty confusing to say the least. In COSO IC (2013), COSO ERM (2004), it refers to something negative: *"The possibility that an event will occur and adversely impact the achievement of objectives."*

COSO ERM (2017) and the ISO 31000 Risk Management Guidelines (from the onset in 2009), on the other hand, use a neutral risk concept. It concerns both positive and negative effects on the achievement of objectives.

What does all that mean? That the use of the term 'risk' is constantly causing problems! The conventional methods focus on things that can go wrong. That is by no means a holistic approach. Decision-making is always about balancing pros and cons, weighing interests and making choices. Think about it: when you start investing, hopefully you are not only concerned with possible losses whilst forgetting about the returns.

On the other hand, if you choose the more modern holistic definition of 'risk', i.e. the neutral concept – including both upside and downside risk - then you lose most of your audience right away. To them, risk is a load of adversity. And that is no surprise since in common parlance 'risk' has a negative connotation.

Because of all this confusion people like Grant Purdy and Norman Marks advocate avoiding the word "risk." They are talking about avoiding "the R word". "Uncertainty management", "expectation management" or "success management" are already better terms. Or how about "value management"? After all, both COSO and ISO indicate that it is all about creating and protecting value.

The big advantage of referring to 'value' is that you realize that terms like 'value', 'result' or 'improvement' as such are meaningless. It implies that you have to clarify first what you mean by them. The meaning of value varies by stakeholder. Some immediately think about money, like share prices and dividends. Others are primarily interested in for example, punctuality, sustainability, equitability or physical safety.

We don't have a science called 'riskology'. What we do have is a self-contained risk management world with all kinds of consultant-recommended practices. Organizations must then integrate these working methods with all their strength into normal business operations. In practice, this is not easy at all and we all can observe this.

According to many experts in the risk management world you have to make all kinds of statements about your risk appetite. These statements are about the types and amount of risk that you are willing to take. But wait a second, can you express risk as an amount?

Risk profiles suggest that you can aggregate risks for convenience purposes. However, there is no separate unit of measure or currency for risk. If you try to aggregate risks based on monetary value, you will soon discover that what you value most in your life is pretty difficult to monetize.

What we also don't always realize is that opportunities and threats aren't things that exist - other than that they are our mental images. They are our thoughts of potential future events,

circumstances and trends. These images are strongly influenced by our personalities, knowledge and experiences.

Moreover, we humans suffer terribly from biases, prejudices and flawed thinking. One could even argue that conventional risk management itself is based on the loss aversion bias. We humans appear to experience the pain of (possible) loss twice as much as the pleasure of (possible) gain.

In practice, risk management is generally implemented qualitatively. Points are awarded to estimated likelihoods and effects. Using values on ordinal scales (such as 1 to 5) for probability and impact. These are the types of scales that are used in opinion polls.

Then people reason: Risk is likelihood times effect. So, they multiply these values into risk scores with the greatest of ease. They then sort those scores in Excel by level – or it's done for them in their risk management application - and that's how they get their top risks.

However, one cannot simply multiply ordinal values. Remember, ordinal values are the ones that are used for rating, for example the number of stars indicating the service level of hotels. In addition, analyses of causes, events and consequences typically assume cause and effect relations. A lot of them are only knowable in hindsight.

Risk quantification is highly dependent on the quality and quantity of the available data and the assumed dependencies between the factors. If the assumptions are no longer valid, then the value of the model expires. Moreover, we shouldn't forget that they're just models. A map is not the area itself that it represents.

Furthermore, and this is really key, in practice it is never about achieving one single objective. Maybe it was true in the old "shareholder value" way of thinking: maximizing the value for shareholders (earnings per share). And risks were mainly seen as threats to earnings potential. We are all familiar with the derailments to which the approach "money as an end" instead of "money as a means" has led.

Decision-making only becomes interesting if there are dilemmas. Then you have to choose. Dilemmas are always about possible positive and negative consequences for competing or even conflicting interests.

Remember your own position as a civilian last year. Your government was promoting with all marketing forces available that everyone gets vaccinated and claimed that those vaccines are safe. However, the contracts with the manufacturers state that the long-term effects of the vaccines are very uncertain. Moreover, these parties do not accept any liability. Not an easy choice to be made.

How about the new insights?

According to the conventional approach there are loads of risks out there. Therefore, you must have separate risk management to manage your risks. To ward off disasters, you must invest in risk identification, risk analysis, risk mitigation and risk monitoring.

This way of thinking was increasingly challenged during the past years. Thought leaders indicated that it is mainly a matter of looking ahead in a consequence conscious way. They emphasized the importance of reconciling dilemmas when making decisions. Making choices is a responsibility that is part and parcel of the daily work of every entrepreneur, director, line manager and project leader.

When making decisions you have to weigh the pros and cons. There is nothing in life with only benefits. There are always drawbacks, too. Take for example buying a home, assuming that you can do that nowadays with ever increasing prices. Obviously, home ownership comes with advantages, such as capital accumulation, more freedom to adjust your house to your personal taste and lower monthly costs than renting.

There are also significant possible disadvantages particularly in case of a mortgage. That is speculating with borrowed money. And think about shitty neighbors you can get or subsidence of the foundation due to changed groundwater levels.

As a management team you will not realize your goals by combating misery and limiting failures. You become successful by seizing opportunities that help you to perform better than expected. And by limiting threats, such as ransomware by cyber criminals!

Periodically updating a list of things that could go wrong is not the same as figuring out how best to achieve your goals. And it is certainly not the same as dealing with dilemmas. It all comes down to making decisions and therefore it is no different from ordinary management: allocating scarce people and resources in order to produce products and services that meet requirements and expectations.

Uncertainty is caused by lack of information. Decision-making is not just about having enough quality information. It is primarily about mentality. As a decision maker you have to weigh possible pros and cons associated with your different options. In other words, you are the one responsible for reconciling competing interests.

Cloud computing brings you scalability, but it makes you dependent on the performance of your supplier. As a decision-maker you have to choose. This is quite different from creating a separate risk management initiative, system or even function. You have to weigh the possible advantages and disadvantages when designing, executing, evaluating and improving your business processes and working standards.

Risk management methodologies underscore the importance of integrating dealing with risks in your regular management system. New insights challenge why you would first create something separate – a risk management system – and then try to integrate it. Constantly looking ahead and making trade-offs is already inherent in your existing management system.

As a decision maker you can very well use the help of critical friends when making your considerations. In other words, you need knowledgeable colleagues who keep you on your toes: decision supporters. Valuable people who help you with using realistic assumptions when making plans, scenarios and forecasts.

These people are indispensable. Marketing is an ingenious profession with sophisticated influencing techniques. You should always be on guard that there are individuals or groups who want to highlight the advantages and mask the disadvantages.

Take for example the 17 Sustainable Development Goals. If you know little about the origins of Agenda 21 and Agenda 2030 these goals sound like a transformation recipe for a wonderful world. However, investigative journalists point out what proponents don't tell you. Namely that achieving the ESG targets is only feasible by implementing draconian measures: digital totalitarianism. This implies that national governments act as the middle management of large NGOs and huge investment funds.

Hence, the importance of people who think constructively and critically, who question and challenge you as a decision maker. And who help you to increase the likelihood of your success.

What can we learn from the new insights?

We have reviewed the development of conventional risk management. It easily degenerates into an illusory separate system. Labelling something as "high risk" doesn't necessarily help those who have to make tough decisions. When you are accountable what you really need to know is: the likelihood of your success.

If you want to add value, realize that it is always about competing or even conflicting interests. And therefore about integrity, about ethics. Take commerce versus compliance. Imagine that your firm could earn lots of money from a wealthy prospect with questionable activities. As a decision-maker you have to choose which interests of which stakeholders are given priority. These are moral considerations. So, at the end of the day it comes down to people's mindset. The key word is not so much leadership, but mentality!

Check which goals are dominant. If only commercial interests predominate, then that is a big red flag! Pay particular attention to matters such as core values that determine which interests should be at the expense of others. Do not look at what you can find on the website, but look at the actual behavior of the managers. Is getting caught the main driver of their compliance practices?

When it comes to dealing with the future there is every reason to remain modest. Our human abilities to understand the future are pretty limited. Opportunities and threats can hardly be objectified in a rapidly changing world. It is a complete illusion that you can figure out in advance what could happen in an environment with so many actors and factors.

Think about the implications of Artificial Intelligence, Internet of Things or even Internet of Bodies: transhumanism. Well, the one thing we know for sure is that your privacy will be gone. Hence you need people who are alert to what is going on. You need a culture in which unwelcome news is also a appreciated. And last but not least you need the flexibility and ability to improvise, for example in case of incidents and innovations.

If your organization is dealing with a supervisory authority that still believes in risk management paraphernalia, start a conversation about the new insights. If that doesn't help, try your best to meet the basic compliance requirements. But spend as little capacity on it as possible. Instead, use your time, energy and attention to help your colleagues make better decisions.

Is risk management redundant? In order to answer that question, would it be possible to talk about the essence of any organization without using the term 'risk'? Let's give it a try:

The key question for every manager or management team is: to which extent is your area of accountability future-proof?

1. How do you become future-proof?
   By continuing to keep your core stakeholders happy.
2. How do you keep your core stakeholders happy?
   By creating and protecting value for them - obviously depending on what they value.
3. How do you create and protect value for them?
   By delivering products and services that meet their requirements and expectations.
4. How do you deliver according to their requirements and expectations?
   By organizing your processes in robust yet flexible ways, as change is constant in life.
5. How do you organize your processes in robust yet flexible ways?
   By having effective working standards and practices; some people call them 'controls'.
6. How do you get effective working standards and practices?
   By analyzing your opportunities and threats in a realistic way. By asking: What-can-

happen and What-if-x? And by analyzing to which extent you are capable of dealing with these situations.

7. How can you analyze your opportunities and threats?
   By weighing the interests of your core stakeholders - when designing, executing, evaluating and improving your business processes and working standards.
8. How can you make sure that the interests are being weighed in an equitable way?
   Ultimately, it comes down to having decision-makers with the right competencies and intentions.

Marinus de Pooter is an independent interim professional, consultant and trainer based in The Netherlands. He focuses is on supporting management teams to remain future-proof. He has developed the value management approach. It aims at dealing with competing interests when allocating scarce resources in pursuit of value creation and protection.

In previous positions Marinus was Director of Finance at Ernst & Young Global Client Consulting, European Director Internal Audit at Office Depot and ERM Solution Leader at EY Advisory. He can be reached at marinus@mdpmct.com and +31 6 5206 2166.