It's all about mentality!

Transcript of the presentation by Marinus de Pooter at the Risk & Resilience Festival at the University of Twente on November 10, 2022.

'Safety doesn't happen by accident' is the theme of this conference. Creating and protecting safety requires coordination and cooperation. In other words: an adequate organizational structure and culture. And when talking about culture, it is about people's behavior, attitude and mentality.

Mentality is the thinking and behavior pattern of a person or a social group. It is what they find normal. Mentality is closely related to their core values: their beliefs and ideals about what is acceptable and unacceptable behavior.

Safety is one aspect of the many challenges and dilemmas that decision-makers face. They must strike a balance between the potentially conflicting interests of their core stakeholders. In practice, commercial pressures often predominate at the expense of safety, sustainability and compliance.

Balanced decision-making requires consequence consciousness. As a decision-maker you need to take a realistic view of the potential pros and cons of your options to act or to refrain from acting. It implies making tough choices under uncertainty. Which interests of which stakeholders do you give priority? Your choices have everything to do with your integrity, morality and mentality.

Are the conventional risk management practices helpful in this respect? Do they help you to make balanced decisions? Or does maintaining the very common risk registers primarily serve compliance purposes? Over the last ten years or so I have come to the conclusion that many current risk management practices have little value outside of the realm of compliance.

Producing lists of risks may help to convince your supervisory authorities that things are 'in control' within your organization. However, they are not of great help when you have to reconcile dilemmas. You probably noticed that the attention gradually has shifted more to decision-making during the past years. To making choices. To balancing pros and cons. To dealing with competing or even conflicting interests. And hence to ethical considerations. Mentality is a key factor in decision-making.

In this session I want to share with you recent insights in dealing with the uncertain future. These are developments with major ramifications for risk managers, compliance officers, safety consultants, privacy specialists, information security officers, business continuity experts, resilience people and internal auditors. To name a few professionals who love to talk about risks all the time.

Before we dive into this let's have a quick look at the differences between safety and security. In short: in order to feel safe you need security.

- Security refers to the protection of organizations, individuals an assets against external threats that are likely to cause harm. The focus is on deliberate threats, e.g. malicious acts by criminals. It is more physical.
- Safety refers to the feeling of being protected from factors that cause harm. The focus is on unintended threats, e.g. an employee slipping in the workplace. It is more emotional.

Safety presents decision-makers with challenges and dilemmas. Think of the safety in a warehouse. When you are the manager you must strike a balance between the competing interests of your core stakeholders. Compliance is one aspect of this. Imagine that the certified forklift driver already has gone home as he wasn't feeling well. Goods need to be loaded and dispatched urgently to an important customer.

Do you allow a non-certified driver to operate the forklift as a matter of professional judgment?

- If things go right, you are an admired pragmatic. Admittedly, you violate the rules, but it is for the greater good.
- If things go wrong, you are an irresponsible manager. Those rules are there for a reason.

The ways people deal with situations like this vary significantly. It works both ways and has everything to do with their personality, attitude and mentality.

- On the one hand, it is very tempting to sit on the safe side: 'better safe than sorry'. Think of the proportionality of measures or the safety margins used.
- On the flipside, certain people are reckless and expect it will all end well. Or they even don't think ahead and reckon that they will improvise through it when things go wrong.

Does conventional risk management help to reconcile dilemmas?

Or does it serve compliance purposes only? Imagine that the 'best before date' on packaged food has expired. The food still smells very edible. Do you believe that eating it is going to adversely affect your health? Are you going to throw it away if wasting food goes against your principles?

Risk management the way it's applied in many organizations can be referred to as 'conventional risk management'. It is a structured approach to deal with the uncertain future. It is aimed at identifying, analyzing, mitigating and monitoring all sorts of things that can go wrong. The underlying thought is that there are loads of risks out there. And you got to do something about them as a management team.

To most risk, safety and security professionals managing risks is part of doing business as much as fireworks belong to New Year's Eye. However, during the past years thought leaders increasingly started suggesting that separate risk management is redundant. To which extent is it helpful to reconcile your dilemmas?

Redundant has different meanings: that there is more than is necessary. Or: that something is not or is no longer necessary. I mean the latter one: is risk management as a separate system or program or function superfluous, inessential, unnecessary? In other words: can you be successful without using the paraphernalia of risk management?

According to many experts, risk management can 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 would help you achieve your goals.

In risk management approaches, people typically check what can go wrong in the future. They make substantial lists of risks: the well-known risk portfolios, risk scenarios, risk registers. Tim Leech and others call this "risk list management".

The risks are usually categorized using a taxonomy. And prioritized using risk scores based on risk criteria for likelihood and effect. Control measures play an important role in this approach. You absolutely need them to mitigate your risks. By the way when you hear the verb 'to migrate' you can be sure you are dealing with conventional risk management.

Periodic reports with information on the 'state of risk' are submitted to the management team and the Board. It is a very common practice and I bet that you recognize this from your own experience.

What if risk management were indeed redundant?

What would be the ramifications of redundant risk management? There are quite a few people working in the risk management world. Think about the people who have been appointed to 'risk owner' by the risk managers. How about all those ideologists who are busy in their organization with finetuning their Risk & Control Self Assessment methodologies. And I'm not even talking about the countless risk consultants and risk management software vendors.

So, you might think: It can't be true that risk management is redundant. But …. if risk management is the answer, what was the question again? How well does conventional risk management help decision-makers deal with uncertainty, disruption and dilemmas? Or is it more of 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. In practice that always involves competing or even conflicting interests. Imagine a producer of PFASs, the synthetic chemical compounds that we all use. These man-made substances are used e.g. in non-stick pans, fastfood packaging and extinguishing foams.

These products are valued by consumers and generate profitable returns for shareholders. However, these are forever chemicals. We can't get rid of these pollutants. They negatively impact our immune systems and cause increased risk of cancer. As a licensing authority you have to choose.

You can pick any other situation whereby 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. To which extent do conventional risk management practices help them to deal with their dilemmas? Do they really need separate risk management?

Suppose that the following applies to the decision-makers in question:

- They look ahead constantly as part of their daily management activities. They seriously ask questions like: 'what-can-happen?' and 'what-if-x?' And they analyze how events and trends could help or hinder the interests of their core stakeholders.
- They show that they are consequence conscious and make realistic estimates of possible positive and negative effects. That is, they consider the potential impacts of their options on the competing interests of their stakeholders.
- They demonstrate that they have proper competences and intentions to weigh the estimated effects on the interests at stake. And they seek to do so in an equitable, fair way. In other words, they have the proper mentality. They appreciate unwelcome information, too. And they realize that when they choose an option because of the estimated benefits, they will have to deal with the associated downsides.

The key question is: Do they need separate risk management in order to make a balanced decision? Or is this all part and parcel of their ordinary management duties?

How did the current risk management practices come about?

In order to better understand the current practices of conventional risk management I invite you to have a look at the origin of the risk registers. They have a lot to do with safety.

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 mainly 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 registers) was gradually seen as a characteristic of good organizational governance. So, you might think: it can't be true that risk management is redundant.

However, those points of interest in the factories 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 had thought about how the safety of the employees could be endangered. And that they had taken appropriate measures to mitigate those risks.

We are still familiar with this phenomenon in the context of the working conditions acts and health and safety audits. So, if you come across a list of risks in e.g. annual plans, team plans and project plans you now know where they come from.

Separate functions emerged dealing with safety, compliance and risk management. A serious side effect of this development is that colleagues quickly think: if you have queries about risks, please don't ask me but contact those experts.

If line managers are only held accountable and rewarded for their commercial performance, then compliance and safety will soon be defeated. You should ask yourself how realistic it is to believe that a bunch of safety, compliance and risk officers can keep the cowboys in your organization on the right track.

Reconciling dilemmas such as commerce versus compliance is all about mentality. You probably also know these people who reason like this: 'If they don't want us to do this then they should ban it.' Or: 'Fines from regulators are just ordinary business costs.'

Due to their role supervisory authorities are hardly interested in the 'upside' of risk. A board member once confided to me that he considered risk management primarily as a compliance matter. To him effective risk management means above all that he doesn't get into trouble with his external or internal supervisory authorities.

Brochures and articles about risk management try to get away from the compliance angle. They argue that in rapidly changing times business people, like sailors, must skillfully navigate turbulent waters. Risk consultants say that understanding and managing risks is absolutely necessary for successful leadership. In their messages you'll encounter the term 'imperative'. It constitutes your business case for implementing risk management.

And during training supervisory board members are taught to ask about the ‘top ten’ risks. That is apparently a sign that people have thought carefully about their vulnerabilities. So, you might think: it can't be true that risk management is redundant.

Internal specialists and external consultants used risk management to help organizations limit their exposures to all kinds of harm and suffering. It led to a variety of methodologies and codifications of best practices: the internal control, risk management and compliance standards.

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

The more these best practices were made mandatory the more lucrative their revenue model became. Extensive maturity models resulted in more and more bells and whistles. Numerous special ERM and GRC applications have been developed. ESG solutions are the latest product line. It's now a multi-million industry with huge commercial interests. So, you might think: it can't be true that risk management is redundant.

It is striking though that you very rarely encounter entrepreneurs, line managers or project leaders at training courses, seminars or conferences like this one. That's quite remarkable, because risk management promises to help them achieve their objectives better. These people are not stupid. If it really helped them, wouldn't they sit in the front rows and learn how to take advantage of the elaborate risk management practices?

In the real world risk management has become 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 a tool to achieve your goals under uncertainty and to reconcile your dilemmas.

What is particularly problematic about conventional risk management?

It all starts with the core concept: 'risk'. Unfortunately, there is no universal definition of the term 'risk'. It is salient that ISO - mind you the international organization for standardization - uses more than 40 different definitions of risk in their own documents.

In common parlance “risk” has multiple meanings:

- the chance of an unwanted event happening;
- the cause of that event, like a risk factor or a risk driver;
- that event itself;
- the consequences of that event, also called impact, implication or effect.

So the term ‘risk’ is already pretty confusing. Do we really know what we are talking about when we mention e.g. ‘safety risk’? In COSO Internal Control (2013) and COSO Enterprise Risk Management (2004) 'risk' refers to something negative: ‘the possibility that an event will occur and adversely impact the achievement of objectives’.

In safety management people associate ‘risk’ with danger and harm. In common parlance 'risk' has a negative meaning as well. ISO 45001 (Occupational Health and Safety Management Systems) and ISO 9001 (Quality Management Systems) talk about ‘risks and opportunities’.

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

Obviously this change has had significant implications. Originally COSO used four so-called 'risk responses': Accept, Avoid, Reduce and Share. COSO added 'Pursue' as the fifth risk response in 2017: 'accept increased risk to achieve improved performance'. This reflects the risk-return balance. However, for the average safety consultant pursuing risk is like swearing in church (or synagogue, mosque, temple).

The lack of clarity of the term 'risk' is constantly causing problems. The conventional approach focuses on things that can go wrong. That is by no means a holistic approach. Decision-making is about analyzing what could help and/or hinder you, about weighing competing interests, about making choices.

Think about it: when you start investing, hopefully you are not only concerned with possible losses but also with returns. And when applying for a job, you are not only concerned with the bad chance that you will get a nasty manager, have an awful work-life balance or that you might get fired easily. You also consider personal development opportunities, supportive colleagues and inspiring assignments.

If you choose the more modern, holistic definition of 'risk', i.e. the neutral concept - including both upside and downside risk - then you lose your audience right away. To them, risk relates to a load of adversity and misery. Because of all this confusion thought leaders like Grant Purdy and Norman Marks advocate avoiding the word 'risk'. They talk about avoiding 'the R-word'. 'Uncertainty management' or 'success management' are already better terms.

I regularly use the term 'value management'. Both COSO and ISO indicate that the purpose of risk management is creating and protecting value. The big advantage of referring to 'value' is that it makes you realize that terms like 'value', 'success', 'result' or 'improvement' themselves are meaningless. You first have to clarify what you mean by them.

The meaning of 'value' varies by stakeholder. Some of them immediately think about money, like share prices and dividends. Others are primarily interested in e.g. physical or social safety, sustainability, social impact, compliance or customer focus.

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. Those working methods must then be integrated into the existing management system. In practice, this appears to be far from easy and we can all observe this.

The ever-expanding risk management jargon adds to the confusion. For example, consulting terminology includes:

- 'risk governance' as something different than your ordinary business governance;
- 'risk culture' besides people's customs and behaviors in your organization;
- 'risk owner' in addition to being in charge of a department, function, process of project;
- 'risk indicators' supplementing your performance indicators;
- 'risk intelligence' alongside your normal business intelligence.

According to many experts in the risk management world you have to make all kinds of statements about your 'risk appetite': the types and amount of risk you're willing to take. 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 images of potential future events, circumstances and trends. Our images are strongly influenced by our personalities, knowledge and experiences.

We humans suffer terribly from biases, prejudices and flawed thinking. Think of the widespread self-overestimation. In addition, lots of people prefer to remain ignorant of risk. Or take self-serving bias. If something went well, we like to attribute success to ourselves. And if things go wrong, it is always due to someone or something else.

One could 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 addition, risk assessments (particularly analyses of causes, events and consequences) assume cause and effect relations. A lot of these relations are knowable in hindsight only.

In practice, risk management is usually implemented qualitatively. Points are awarded to estimated likelihoods and effects using values on ordinal scales (for example, from 1 to 5 or 6 or 10). Then people reason: risk is likelihood times effect. So, they then multiply these scores for probability and impact into risk scores with the greatest of ease.

Thereafter they sort those values in Excel by level. Even better, it's done for them in their risk management application. And that is how they get their top ten risks. However, you cannot simply multiply ordinal values. These are the ones that are used for rating purposes e.g. the number of stars to indicate the quality of hotels.

Those scores are often plotted in a 'heat map', the Probability Impact Diagram or Probability Consequence Diagram. For many people this is the true symbol of risk management. With two axes: for likelihood and effect. With colors per cell of the matrix. Since these heatmaps are very misleading avoid them as much as possible.

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 the value of the model expires. And 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 reality it is never about achieving one single objective. Maybe it was in the old 'shareholder value' way of thinking: maximizing the value (earnings per share) for the shareholders. In this context 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 about possible positive and negative consequences for competing or even conflicting interests under uncertainty.

Remember as a citizen the situation you were in last year. Your government is promoting with all marketing forces available that everyone gets injected multiple times. They assure you that the vaccines are safe and effective. They don't tell you that the contracts with the suppliers state that the long-term effects of the vaccines are uncertain.

Moreover, the vendors do not accept any liability. Scientists who challenge the safety and effectiveness claims are cancelled. You aren't updated on the adverse effects occurring. Anyone who dares to doubt the official narrative is deplatformed on social media. And if you don't comply you are treated as a pariah. Not an easy choice to be made….

How about the new insights?

In the Anglo-Saxon planning & control world the idea of manufacturability of life is rampant. Risk management and internal control approaches naturally fit in well with this DNA of makability. If you know what you want, cleverly think of what might go wrong, implement suitable control measures and get evidence of their effectiveness, then reality will unfold itself as anticipated.

This is the so-called 'ORCA'-world: Objectives-Risks-Controls-Assurance. The approach easily turns into an illusory control world in which unplanned success is just about the worst thing that can happen. According to the conventional approach there are loads of risks out there. Numerous things can go wrong, for example regarding safety. Therefore, you'd better have a separate safety risk management system to manage these risks. To ward off disasters you must invest in risk identification, risk analysis, risk mitigation and risk monitoring.

The conventional approach was increasingly challenged during the past years. Thought leaders indicated that it is mainly a matter of looking ahead in a consequent conscious way and of reconciling dilemmas. This responsibility is part and parcel of your daily work as a decision-maker.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. Evidently, home ownership comes with significant 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 the possibility that you get shitty neighbors or subsidence of the foundation due to changed groundwater levels.

The same goes with capacity. It does not make a lot of sense to only ask about the potential negative consequences of overcapacity or undercapacity. Okay, you'll have less returns on your assets and you'll have to say no to your clients. However, both situations also have potential positive effects. Overcapacity means that you can easily serve new clients if their current suppliers have run out of capacity. And undercapacity could imply scarcity in your market justifying higher rates.

As a management team you will not be successful by combating misery and limiting failures. You become successful by seizing opportunities that help you to perform better than expected. And by limiting your threats such as exposure to 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. Therefore, it is about ordinary management. That is basically about allocating scarce people and resources in order to produce products and services that meet requirements and expectations.

Effective decision-making is not just dependent on the availability of suitable information. It is primarily about mentality. As a decision-maker are you are responsible for dealing with competing or even conflicting interests. You have to weigh possible pros and cons associated with your different options.

This is quite different from creating a separate risk management initiative, system or even function. As a decision-maker you have to choose. You have to weigh the possible advantages and disadvantages when designing, executing, evaluating and improving your business processes. You'll easily recognize the well-known PDCA cycle here.

Why would you first create something separate - a risk management system - and then try to squeeze it into your regular management system? Constantly looking ahead and making trade-offs is already inherent to your regular management cycle which is aimed at increasing the likelihood of your success.

As a decision maker you can really use the help of 'critical friends' when making your considerations. In other words, you need decision support from knowledgeable colleagues who keep you on your toes. Who support you with producing realistic plans, scenarios and forecasts. And who help you with using realistic assumptions.

Marketing is an ingenious profession with sophisticated influencing techniques. You should always be on your guard. There are people who highlight the advantages and mask the disadvantages. Always ask yourself: who does benefit from me believing this message?

Take for example the 17 Sustainable Development Goals. If you do not know a lot about the origins of Agenda 21, Agenda 2030 and the New World Order, these SDGs sound like an excellent recipe for a wonderful world. However, investigative journalists point out what the proponents do not tell you about this 'Happy Land'.

The SDGs are the marketing version of the technocracy movement. In the last century the choices of the politicians had let to the Great Depression. A group of scientists, technicians and bureaucrats concluded that allocating the world's resources should better be left to people like themselves.

Achieving these SDGs will only be feasible by implementing draconian control measures fueled by fear and guilt. It requires a structure whereby the countries' governments act as the middle management of corporate states like BigTech companies, of huge investment funds like Blackrock and Vanguard, and of powerful NGOs like the UN and the WHO that is funded by very wealthy people.

Hence, the importance of people who think constructively and critically, who help you with your blind spots and who challenge you as a decision-maker. Ultimately, they help you to increase the likelihood of your success.

What can we learn from the new insights?

We have reviewed the characteristics of conventional separate risk management. It easily degenerates into an illusory system. Labelling something as 'high risk' does not necessarily help those who have to make tough decisions. If you are accountable what you really want to know is the likelihood of your success. The likelihood that your products and services are going to meet the requirements and expectations of your core stakeholders.

According to the new insights as a management team you should focus on your impactful decisions. Ask the essential questions: 'What-can-happen?' and 'What-if-x?' And reflect on your own attitude, behavior and mentality:

a. To which extent do we look ahead sufficiently?
b. Do we consider the possible implications for the interests of our stakeholders?
c. Do we make explicit and discuss the assumptions used in our plans, budgets, proposals, forecasts, and so on?
d. Do we realize the level of uncertainty in our estimates?
e. Are the right experts involved in our assessments?
f. Do we allow enough room for critical voices?
g. Are we sufficiently conscious of the potential consequences of our choices?

h. Do we understand to which extent our strengths and weaknesses are going to enable us to benefit from our opportunities and to cope with our threats?
i. If we choose for an option because of the perceived advantages, do we bother about the potential associated disadvantages, too?

Always discuss which goals are dominant. If only commercial interests predominate then that is a serious red flag! Pay particular attention to the 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 behavior of the executives and managers. If getting caught is the main driver of their compliance policy then that is a real issue.

It remains remarkable that many people think that risk management is about updating risk lists. Stop making risk inventories for the sake of inventorying risks. Quit updating risk registers every quarter or year. Nobody uses them whenever important decisions have to be made.

Do not spend endless time measuring risks. Because it is not about risks at all, but about estimating the likelihood of your success as an organization(al unit). And avoid jargon as much as possible. Don't use words starting with 'risk'. Use ordinary business language, or even better common language.

There is every reason to remain modest. Our human abilities to fathom the future are limited. Realize that opportunities and threats can hardly be objectified in a rapidly changing world. It is impossible to figure out in advance what could happen in a world with so many actors and factors. That is a complete illusion. Think about the implications of Artificial Intelligence, Internet of Things or even Internet of Bodies (transhumanism). The one thing we can expect with certainty is that our privacy will be gone.

If you want your organization(al unit) to survive and thrive, make sure that you have:

- experts who are alert to what is going on;
- 'critical friends' who keep the decision-makers on their toes;
- a culture in which unwelcome news is appreciated;
- committed people who are able to improvise.

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

The new insights indicate that you should not focus on managing risks. Instead focus on creating and protecting value for your core stakeholders. Their satisfaction is the decisive condition for your organization to remain future-proof.

Marinus de Pooter is an independent interim professional, consultant and trainer. He focuses is on supporting management teams to remain future-proof (www.stay-future-proof.com). In previous positions Marinus was Director of Finance at Ernst & Young Global Client Consulting, European Director Internal Audit at Office Depot and regional ERM Solution Leader at EY Advisory. He can be reached at marinus@mdpmct.com and +31 6 5206 2166.