Stop managing risks!

Transcription of the presentation at the Risk & Resilience Festival (University of Twente) on November 7, 2024

Marinus de Pooter

1. Introduction

If you are a professional who can't talk for five minutes without using the word 'risk' a title like this immediately raises your eyebrows. It even makes your neck hairs stand up or your hair stand on end.

According to many risk professionals, managing all sorts of risks belongs to doing business like snow to winter sports. This presentation focuses on captivating insights regarding conventional risk management practices.

I work as an interim manager, consultant and trainer. Typically, people I meet find stopping to manage risks super stupid. Organizational leadership must do something about risk. Period. This is the underlying principle in the international standards for risk management like ISO 31000 and COSO ERM.

According to many experts and their followers, risk management can and should be implemented. According to them, it is very unwise not to do it. Managing risk saves you from unnecessary pitfalls and above all it helps you achieve your goals. In recent years, however, the understanding of dealing with uncertainty has changed significantly.

Managing risk involves quite a few people. In the world of risk management, they are assigned all sorts of roles. Think of those designated as 'risk owners' by their Risk Management colleagues. Still others make their living as internal risk managers, risk officers and risk analysts. Not to mention the countless external risk advisors and software vendors.

Risk consultants keep selling them and many organizations keep buying them: risk frameworks, risk policies, risk workshops, risk registers, risk dashboards and so on. These tools are typically designed to identify, analyze, mitigate and monitor individual risks or individual risk categories.

Executives are expected to consider what keeps them awake at night. In practice, based on this information hefty lists are maintained: risk registers. Tim Leech and others call this approach 'risk list management'. To find the most important risks, great importance is placed on completeness. Imagine forgetting a risk that could be important. As a result, those risk lists become long and wide: easily 20 columns in a spreadsheet.

The underlying belief is that the ultimate goal is to mitigate calamities and combat woes. However, in his book 'Guide to effective risk management' Alexei Sidorenko points out that it is not about managing risks, but about making better decisions.

If risk management is the answer, what was the question again? How well do conventional approaches help decision-makers deal with uncertainties, disruptions and dilemmas? Or is it more of a belief system? Could there be missionaries, believers and inquisitors who have serious commercial interests in maintaining this ecosystem?

The developments I'm going to take you through are as follows:

- from managing individual risks and warding off possible calamities;
- via making decisions under uncertainty and estimating the likelihood of success;
- to weighing stakeholder interests and reconciling dilemmas.

We will discover that the latter is mostly about the mentality of those making the choices and trade-offs**.**

2. What does 'managing risk' typically mean in practice?

The Three Lines Model is very popular. At least among internal auditors because of the justification for their own independent position. It is an internal management system for clarifying 'risk ownership'. That is, who is responsible for managing risks.

The first line is supposed to manage the risks. They are the executive branch. The second line is formed by specialists who understand compliance and risk management. They are the legislative power, the architects of the internal control system. Internal audit is the third line, acting as the judiciary, passing judgment on what comes of the efforts in practice.

In addition to expertise, the second line is supposed to offer support. This should involve rolling up their sleeves and helping to translate policies into procedures. In practice, however, they often limit this to flinging established policies over the fence.

Some believe that the second line also has an inspection role: monitoring compliance and holding accountable are considered part of their tasks. In practice, this model mostly creates hassle about who does or does not belong to which line and what they should or should not do.

COSO ERM (2004) defined risk management as: "a process designed to identify potential events that may affect the entity ... to provide reasonable assurance regarding the achievement of objectives".

Other standards like ISO 27001 are also about having to conduct a risk assessment to identify potential threats. Subsequently, you have to implement control measures to mitigate them. And to conduct reviews and audits to establish that they remain effective.

This is referred to as the 'ORCA' approach:

- Objectives, setting goals;
- Risks, identifying things that can go wrong;
- Controls, implementing adequate control measures;
- Assurance, obtaining assurance by checking control effectiveness.

The promise is that it increases the likelihood that the future will unfold as expected. The idea of makeability reigns supreme in the planning & control world. Risk management fits this DNA perfectly.

An important observation is that COSO ERM (2017) no longer views risk management as a process, but as: "the culture, capabilities and practices that organizations rely on to manage risk".

In practice, individual risks are usually categorized using a taxonomy. And prioritized using risk scores, using scales for likelihood and effect ranging from 1 to e.g. 5 or 6 or 10.

Controls play an important role in this approach. Namely, they should 'mitigate' the risks. When you hear or read that verb you know that you're dealing with conventional risk management. Obviously, assessing controls requires that you make all sorts of assumptions about their adequacy and effectiveness.

Periodic reports are produced for management and supervisory authorities. They receive information about the 'state of risk'. Insight is given into the degree of exposure to all kinds of possible calamities and woes.

This is a widespread approach. Imagine you are a line manager. Staff officers are supposed to help you to make better decisions. Instead, in reality they come to collect information from you that you then can read back in their reports.

Dealing with uncertainty is inherent in everyday management. There is no management without uncertainty. Decision-making is about analyzing multiple options and weighing potential pros and cons for what core stakeholders value. Suppose you start investing, you are naturally concerned not only with potential losses but also with potential returns.

Does formal risk management have any value other than reassuring supervisors? Other than keeping them happy, is there anything in risk management that is not already part and parcel of day-to-day management?

Does it make sense to first develop and implement all kinds of risk management attributes (such as risk registers, risk treatment plans, risk reports et cetera) and then try to integrate these paraphernalia into the existing management?

Or is this more logical?

- To forget about 'risk management' altogether - apart from compliance purposes;
- to take the perspective of the decision-makers and their dilemmas as a starting point;
- to actively help them deal with dilemmas and manage the expectations of their core stakeholders.

Before we dive into this in more detail, let's take a quick look at where conventional risk management comes from.

3. What are the origins of conventional risk management practices?

The insurance industry played a distinguished role. They helped customers protect themselves from potential misery. They sell policies that focus on insurance against possible quantifiable calamities.

As early as the 1960s, the first Securities and Exchange Commission requirements emerged for the inclusion of risks in documents in the context of IPOs. At the beginning of this century came requirements to include them in annual and quarterly reports.

These involve factors that make shares speculative for shareholders. All aimed at preventing financial losses for those involved. From this arose the requirement to have a Risk Management Framework: a coherent set of risk identification, analysis, mitigation and monitoring.

Internal specialists and outside consultants used risk assessments and treatments to help organizations mitigate unwanted outcomes. This led to methods and codifications of best practices.

In the 2004 edition of the COSO ERM Framework, risk management was seen as a process. If you hadn't already implemented it, consultants including myself were lining up to help you.

Comprehensive maturity models resulted in more bells and whistles. Over time, numerous dedicated ERM, GRC and ESG applications were developed. The more risk management practices became mandatory, the more lucrative the revenue models became for those consultants. It is now a multi-million dollar industry with big stakes.

Over the years, risk management has increasingly been treated as a stand-alone process and function. In the financial sector, legislators and regulators even came up with a risk management function to be independent of management. This function has a sheriff-like role with the goal of keeping certain cowboys on the straight and narrow. It must inform management based on its own risk assessments.

By the way, you have to wonder how realistic it is to think that with a bunch of risk and compliance officers you can keep the real cowboys in line. If sales representatives are rewarded only for their commercial performance, compliance and morality will soon lose out.

No doubt you know people with this mindset:

- "If they don't want us to do this, they should ban it."
- "Fines from regulators should be viewed as operating expenses."
- "As long as we haven't been caught, we haven't done anything wrong officially speaking."

To understand current risk management practices we must also go back to the origins of risk registers as the basis for the common 'heatmaps'. Risk inventory lists became commonplace in factories in the 1970s. There they had begun to use lists with a variety of concerns regarding worker safety.

As more and more regulations in this area came in, these lists were used primarily to draw attention to potentially dangerous situations. These lists soon took on a compliance function: they were useful to inspectors who came to check on companies.

Governments, regulators and supervisory authorities then embraced these practices as methods of demonstrating that organizations have their affairs in order. They expect internal inspectors to review lists of risks. 'Doing risk management' (read: keeping those risk lists and naming top risks) gradually became seen as a hallmark of good organizational governance.

4. What is problematic about conventional risk management?

Recent insights underscore significant problems with risk management. Roger Estall and Grant Purdy, in their book Deciding, conclude that it is a millstone hanging around the necks of organizations that they would be better off getting rid of.

It starts with the core concept of 'risk. So what are we actually talking about? Unfortunately, there is no universal definition of it. Notably, ISO - mind you the international organization for standardization - uses more than 40(!) different definitions of risk in its documents.

When people use the word 'risk', they can be talking about different meanings:

- the likelihood of an (undesired) event;

- the cause of that event, also known as 'risk factor' or 'risk driver';
- the selected event itself;
- the consequence of that event, also called 'impact' or 'effect.

Still others mean by 'risk': the volatility of expected outcomes.

Causes and effects are themselves events. All of life consists of occurrences, circumstances and trends that interact. Consequently, experts point out that risk is not about events occurring, but rather about the relationships between events.

In COSO IC (2013), COSO ERM (2004) and, for that matter in common parlance, 'risk' refers to something negative: possible loss. Something that could cost you money, be bad for your health or bring you into disrepute. Risk is then the measure of the likelihood and severity of adverse effects.

The ISO 31000 Risk Management Guidelines (from its inception in 2009) and its major competitor COSO ERM (2017) use a neutral concept of 'risk'. It involves both positive and negative effects on achieving objectives. Risk then is an uncertain consequence of an event or activity related to something that people value.

This change has far-reaching implications. Originally, COSO used four so-called risk responses: Accept, Avoid, Reduce, Share for potential misery. In 2017, COSO added Pursue as a fifth risk response: accept increased risk to achieve improved performance. This is more in line with the common concept of the risk-return balance.

According to COSO, Internal Control is a process that provides reasonable assurance regarding the achievement of objectives. Their definition of 'opportunity' was: "the possibility that an event will occur and positively affect the achievement of objectives". They took a fatal turn in 1992 by indicating that opportunities are not part of internal control, but must be funneled back to the objective-setting process.

The fact that 'risk' has very different meanings implies that simply using the term is already a source of confusion. The traditional focus is on what can go wrong. This is certainly not holistic. Success depends on taking advantage of opportunities as well as mitigating threats.

For example, when you apply for a job, you are not only concerned with the bad chance of getting an annoying supervisor and being fired, but also with personal development opportunities and supportive colleagues.

In contrast, if you use the neutral definition, which implies both upside and downside risks, you immediately lose most people in your audience. To them, 'risk' has a negative connotation.

Because of this confusion several thought leaders suggest avoiding the 'R-word. Alternatives such as 'uncertainty management', 'success management' or 'expectation management' are already better terms. The same goes for 'value management'.

After all, both COSO and ISO state that the purpose of risk management is to create and protect value. It takes into account that different stakeholders value different things, such as safety, profitability and punctuality.

According to ISO 31000, risk management is effective if it is part of decision-making processes. In reality, decision-makers must make choices under uncertainty and reconcile dilemmas due to conflicting interests. It requires dependence awareness, consequence consciousness and clear core values.

Risk management is characterized by a very comprehensive jargon. For example, some say you need to have 'risk dialogues' with your colleagues. Other examples include:

- 'risk governance', while you have already defined tasks, authorities and accountabilities in your business;
- 'risk culture' in addition to existing norms, values and behaviors;
- 'risk owner' while you have already made people accountable for achieving results;
- 'risk intelligence' alongside your existing business intelligence;
- 'risk reporting' while, if all goes well, you already include forecasts in your regular management reports.

The big downside of all this jargon is that ordinary people think: this seems to be about something completely different from my daily work; apparently, dedicated experts are needed for this.

An independent separate Risk management department leads to colleagues quickly thinking: if you have questions about risks you should go to those specialists, because they are the ones. It is inducive to making the intended integration of risk management in business management out of control.

We should talk a little about those 'risk managers'. Management is about allocating scarce people and resources to produce products and services - through policies, processes and procedures - that meet requirements and expectations. Risk managers do not manage. They facilitate, analyze and report.

Conventional approaches focus on reducing individual risks or risk categories to an acceptable level through control measures. If it appears that a manager has accepted a level of risk that exceeds the organization's risk appetite, the issue need to be brought to the attention of senior management.

The 'risk appetite statement' is one of the crown jewels of conventional risk management. According to COSO ERM it is about the types and amount of risk that an organization is willing to accept in pursuit of value.

Risk profiles suggest that you can aggregate all kinds of different risks for convenience purposes. But wait a minute. What are we actually talking about with 'amount of risk'? Do we have a suitable unit of measurement for it?

Saying you have a low risk appetite may sound cool or reassuring, but it has little practical meaning. What exactly does 'low' mean and how do you know if your actual risk exposure is indeed 'low'? Risk appetite statements are meant to help decision-makers avoid causing more adverse effects than they can afford. But do they in practice?

Risk appetite statements are mostly based on the negative definition of risk: potential trouble. At best, the concept of 'risk appetite' works somewhat for financial considerations, such as providing insurance or loans. Those services can be expressed in monetary terms. In the case of compliance or safety objectives, it's a different story.

Talking about how much loss you are willing to accept should always be considered in conjunction with the potential benefit that comes with it. It is about value creation as well as value protection. Therefore, risk awareness is a more beneficial concept than risk appetite.

Consider a practical dilemma in a distribution center. Suppose you are in charge. Then you have to find an acceptable balance between the clashing interests of key stakeholders. Think commerce versus safety.

The certified forklift drivers have already gone home. Goods need to be loaded and shipped urgently for an important customer. Will you allow a non-certified driver to operate the forklift? How well do conventional risk management practices help in making professional trade-offs here?

If it ends well, you are an admired pragmatist. Granted, you're breaking the rules, but it's for the greater good. Necessity knows no law. If things go wrong, you are an irresponsible manager. Those rules are there for a reason.

Risk appetite statements are static, while reality is dynamic. One moment it may be prudent with the available knowledge to take a risk, while a few weeks later it may not be the case. It is pointless to try and mitigate a list of risks regardless of the potential benefits in terms of meeting objectives. What matters is the risk-reward balance.

Tolerance is a better term: the acceptable performance variability. The essential question then becomes: are the estimated values of our KPIs going to stay within the bandwiths of acceptable outcomes in the coming period?

What else is problematic about conventional risk management? We may not always realize that 'opportunities' and 'threats' are our mental images of possible future events, changes in circumstances and trends. These images are strongly influenced by our personalities, knowledge and experiences. Moreover, we humans suffer terribly from biases as Daniel Kahneman and others have pointed out.

There is no science called 'riskology'. What we do have is a self-contained risk management world with all sorts of practices recommended by consultants. Those practices must then be integrated into the existing management system. Unfortunately, the chances of encountering success stories are virtually nil.

In practice, risk management is often approached qualitatively. Risks are then described in words. As opposed to quantitative approaches where risks are expressed numerically. A hybrid form is assigning points to estimated probabilities and effects with values on ordinal scales (for example, ranging from 1 to 5). These scales are also used, for example, in opinion polls or to express the quality of hotels with a number of stars.

If you are asked to name the 'top risks', a risk register is useful. With the greatest of ease Excel multiplies the assigned values for likelihood and effect. Or your fancy GRC application does it for you. Sorted risk scores then provides you with the requested list.

The scores for likelihood and effect are often plotted in the very familiar heatmap. This Probability Impact Diagram is for many the symbol for managing risks. With two axes: for probability and impact.

This nice and visual tool appears to be rather tempting because simple: green is right and red is wrong. You'd better stop using it right away though, as it's a misleading tool. Here are some points to be aware of.

1. The whole focus on individual risks or risk categories is inappropriate. What matters is the expected degree of achieving objectives. Or better yet, finding a balance between competing interests.
2. It is a serious oversimplification of reality. The points in the grid suggest an exactness that does not exist.
3. Single points are assumed. However, risks are distributions: sets of possible outcomes, each with a given probability.
4. It focuses on negativity, while success depends on seizing opportunities as well as mitigating threats.

5. Ordinal series (like from '1' to '5') for likelihood and for effect don't have fixed intervals - in contrast to nominal ones. Hence, calculating risk scores by multiplying the estimated values doesn't make a lot of sense.
6. It is hugely subjective and not data-driven. We humans are especially lousy at estimating probabilities due to our biases.
7. Assessing risks using colors and terms such as 'rarely' or 'possibly,' let alone 'high,' 'medium,' and 'low,' is completely arbitrary and a road to no avail.
8. It deals with individual risks or risk categories and interdependencies are ignored.
9. It remains unclear what impact the plotted risks in the grid have on the achievement of which objectives.
10. The risks in the upper right corner, the 'red risks' with high likelihood and severe consequences, are called 'phantom risks'. High probability means that something happens often and high impact implies game over: going belly up on a weekly basis.

Quantitative approaches attempt to express uncertainty using numbers (such as cash flow at risk, earnings at risk and value at risk). This may be useful in specific cases. If you try to express risk based on monetary value, you will quickly discover that what you value most in your life is difficult to express in monetary terms.

A pitfall is to think that quantitative analyses are objective and superior and that qualitative analyses are subjective and inferior. Risk quantification depends heavily on the assumed parameters in the model and on the quantity and quality of the available data.

If the assumptions used are no longer valid, the value of the model expires. Moreover, they remain only models - not reality itself. A map is not the area it represents. In addition, often you don't even have the time and information to build adequate models.

As the issues become larger and more complex, not only do the uncertainties increase, but so does the subjectivity. After all, there are countless actors and factors that can affect what might happen. You can never include them all in your model. The complexity soon exceeds our human capabilities. Personal visions and opinions then begin to largely determine probability, impact and urgency.

Further, in practice it is never about one objective. Admittedly, perhaps in the old shareholder value thinking. Risks were seen primarily as threats to earnings potential. We have all witnessed the derailments to which the 'money as an end' rather than 'money as a means' approach has led.

Please don't assume this is especially common in commercial environments. In municipalities, for example, the money-driven planning & control cycle seems to be their primary process. If you perform low but stay nicely within your budget, you have fewer issues than if you exceed your budget doing meaningful things for citizens.

Some thought leaders indicate that risk management should be primarily concerned with modeling and quantification. Think business cases, simulations and forecasts. The question is how useful they are if tough real life choices have to be made and ethical dilemmas reconciled.

Because of their role, regulators are hardly interested in the upside of risk. Their job is to minimize the downside. For executives, effective risk management primarily means having no hassle with their external or internal supervisors.

For understandable reasons, they tend to see risk management primarily as a compliance issue. It goes on and on. For example, the new Corporate Sustainability Reporting Directive requires organizations to report extensively on sustainability risks.

Commercially speaking, the ESG circuit (or: circus) is extremely lucrative. A real compliance gold mine. You first make a lot of sales on drafting the standards. Then advising on the implementation makes hefty money. And finally auditing compliance becomes a fixed revenue stream.

Risk consultants try to escape this compliance focus. In rapidly changing times, they argue, business people must effectively navigate turbulent waters as helmsmen. Understanding and managing risk is therefore necessary for effective leadership. Hence the business case for implementing risk management.

During training sessions, board members are taught to ask about the 'top ten risks'. This is apparently a sign that management has properly assessed their main risks. That they have thought carefully about the organization's vulnerabilities as a basis for taking appropriate action to mitigate them.

What is remarkable, however, is that you rarely encounter business owners, line managers or project leaders at risk management trainings, webinars and conferences. This is rather striking, since standards promise that managing risks will enable them to better achieve their goals. Most of these people are not stupid. If it would really help them, wouldn't they all be sitting in the front row eager to learn how to benefit from it?

The reality is that risk management has become an accountability tool. That is very different from a tool for trying to achieving goals under uncertainty. To what extent do common risk management practices really help decision makers deal with their dilemmas?

5. What is the essence of the new insights?

Recent insights assume the perspective of decision-makers. They should focus not on managing risks, but on managing the business, on managing the expectations of their core stakeholders.

It's about achieving organizational goals under uncertainty. What decision-makers need to know is: what is the likelihood of my 'success'? Defined as: delivered performance that leads to the satisfaction of the core stakeholders.

Think employees, customers, shareholders - in this order of importance according to Richard Brandson. If the stakeholders do not remain satisfied with the effects of the organization's performance on what they value, it is not future-proof.

Being concerned with the future implies anticipation and making assessments. It requires asking honest questions such as:

- On whom or what are we especially dependent?
- What are the possible consequences of our choices?
- How realistic are the assumptions in our plans?
- How likely is it that we will be able to achieve our goals?

If the forecasts indicate that the estimated probability of success is low, decision-makers should come up with possible alternatives. If the alternatives are limited, they should consider how to best inform their core stakeholders in a timely manner.

Objectives alone won't get you very far. You have to start doing something. That means making choices about where to deploy your scarce people and resources. If enough time is available, you can do this as comprehensively as possible. However, often you will find yourself navigating in the fog.

People and resources are deployed in the managerial, primary and supporting processes. Practically speaking, processes are about who does what why when where using which tools and applications. Choices have to be made when designing, implementing, evaluating and improving the business processes.

This is no different from the PDCA cycle, from day-to-day management. That is already complex enough. So, why go doing something else besides that, called 'risk management', if not required by a regulator?

Organizational objectives express what core stakeholders value. Different interested parties value different things. Hence, decision-makers have to deal with competing interests under uncertainty. The focus then shifts to the quality of the choices when dealing with dilemmas. The goal is to help them look ahead in a dependence aware and consequence-conscious manner.

As a decision-maker you should be concerned with future-proofing. This is about continuity both in the longer and shorter term. Being able to continue to exist, resilience, means that your organization must be able to withstand a bump. Think digital robustness. It requires flexibility, agility and the ability to improvise.

Estimating uncertainty is pretty tough. The future is unimaginably unpredictable. Under these circumstances you should try to make balanced decisions and timely adjust them when necessary. How much does producing reports on risk levels help you to create and protect value?

Sometimes there is more time and more extensive studies can be done, including quantitative analyses. Often there is limited time available and as you have to make decisions based on your gut and intuition.

There is nothing in life that only comes with advantages. There are always potential or actual disadvantages as well. As a decision maker, you must weigh the estimated pros and cons of your various options to act and to refrain from acting.

Take for instance buying a home. Homeownership not only brings benefits, such as wealth accumulation, more freedom to customize it to your own taste and lower monthly costs than renting.

It is essential to consider the potential downsides as well. Essentially, if you have a mortgage loan, you are speculating with borrowed money. You may also find yourself in the unfortunate situation of having to deal with sagging foundations or horrible neighbors.

Periodically updating a list of things that can go wrong is not the same as figuring out how best to achieve your goals under uncertainty. Norman Marks emphasizes the importance of focusing on increasing the likelihood of success, for example, in his book 'Risk Management in Plain English: A Guide for Executives'.

Balanced decision-making requires that unwanted information be taken into account, too. Marketing is an ingenious profession with powerful influencing and framing techniques. As a decision maker, you have to be aware that people mark the advantages and mask the disadvantages. As a professional, but obviously also as a human being, you should always ask yourself: who benefits from my taking this for true?

Separate risk management easily degenerates into an illusory compliance-driven system. Why set up a separate risk management system first and then try to integrate it into your existing management system? I haven't come across any success stories in the past 20 years.

It remains remarkable that many practitioners still believe there is value in updating risk inventories. The same goes for spending endless time reviewing 'risk levels'. Instead of focusing on 'risk status,' executives should be concerned with increasing the likelihood of performing in line with the expectations of key stakeholders.

It is much wiser to start from the decision-makers' perspective. What they need to know is the probability that they will be able to create and protect what their key stakeholders value.

- It is not about managing individual risks.
- It is not about better meeting singular organizational goals.
- It is about dealing with conflicting interests of core stakeholders when reconciling dilemmas.

'Critical friends' are invaluable for executives. They can support them in stopping managing risks and in starting managing expectations. Please refer to the appendix for practical considerations on how they can help them make better grounded and balanced decisions.

6. Wrap-up

Conventional risk management practices are focused on keeping individual 'risks', 'risk events' or 'risk categories' at acceptable levels. Take for example the 'risk treatment plans' in ISO 31000. To which extent do these paraphernalia help decision-makers to manage the expectations of their core stakeholders?

Risk management approaches serve primarily to reassure regulators. Tools like risk registers and heatmaps are meant to present the 'state of risk' for the top risks. In practice, risk management serves as an accountability instrument in the context of fighting miseries. It thrives in a compliance-driven context. Apart from that, it is redundant as a separate discipline.

'Risk management' and 'management of risk' are pleonasms. Similar to 'spectators present', 'burning fire' or 'open vacancy'. There is no management or decision-making without - implicitly or more explicitly - considering potential positive or negative impacts (on the value to be created or protected) for the stakeholders.

There is no management without dealing with uncertainty. Ordinary management is already tough enough. If not prescribed, don't go rigging something separate called 'risk management'. No one consults risk appetite statements, risk treatment plans and state of risk reports when impactful decisions need to be made.

Considering and dealing with the potential positive and negative effects of uncertainty on objectives is endemic to business management. Every professional executive does this on a daily basis. They don't need something separate called 'risk management' to deal with this.

Decision theory specialists, forecasting experts, statistical planning geniuses, trendwatchers and dilemma coaches can be beneficial for executives struggling with making balanced choices under uncertainty.

It is never possible to predict in advance what might happen in a world with so many actors and factors. That is a complete illusion. Hence the necessity to develop and maintain the improvisational skills of teams.

There is every reason for humility. Our human ability to predict the future is painfully limited. In hindsight, (un)favorable results always remain a combination of (un)wisdom and (un)luck.

About the presenter

Marinus de Pooter is an independent interim professional, consultant and trainer. He focuses on supporting leadership teams in remaining future-proof through dependence aware and consequence conscious decision-making. Marinus was previously Director of Finance at Ernst & Young Global Client Consulting, European Director Internal Audit at Office Depot and ERM Solution Leader at EY Advisory. Please refer to his LinkedIn profile for more details: nl.linkedin.com/in/marinusdepooter.

Appendix | Practical considerations about the critical friend

The role of the critical friend is to help executives to make better grounded and balanced decisions. Based on the recent insights here are a few tips for transition assistance:

1. From putting lots of energy into doing things to avoid failure
   to focusing on what needs to be done to succeed.
2. From focusing on fighting trouble
   to turning the focus to achieving objectives under uncertainty as best as feasible.
3. From bothering colleagues with updating risk lists
   to worrying about information for balanced decision-making.
4. From producing lists of possible calamities
   to providing them with information about possible pros and cons of their options and about possible alternative routes.
5. From treating risks as ends in themselves
   to viewing opportunities and threats as means of estimating possible deviations from future performance and acting on them.
6. From maintaining risk registers for the purpose of risk reporting
   to weighing possible pros and cons in impactful decisions.
7. From aiming for one overarching risk management methodology
   to helping them with practical tools to deal with opportunities and threats in their specific situation.
8. From creating a separate function or committee to deal with all kinds of risks
   to ensuring that the necessary experts actively help to make key choices.
9. From naming separate 'risk owners'
   to creating ownership for results, as that is what is needed to be successful.
10. From creating separate risk management policies
    to creating awareness that every policy area is about dealing with uncertainty.
11. From formulating all sorts of risk appetite statements
    to estimating the extent to which the results achieved will remain within the tolerances of the objectives.
12. From keeping extensive risk lists
    to having the right conversations about the assumptions in proposals, plans and forecasts.
13. From worrying about risk scores and risk levels
    to focusing on the likelihood of achieving key objectives and taking adequate measures.
14. From assuming straightforward relationships between causes and effects
    to realizing that many future developments are inherently chaotic and unpredictable.

15. From conveniently ignoring the enormous complexity of the future
to becoming aware of the dependence on numerous actors with their own interests.

16. From endlessly deliberating on determining probabilities
to realizing that people are lousy at estimating likelihood.

17. From managing risks or risk categories individually
to paying attention to the importance of dependence awareness and consequence consciousness.

18. From building and testing extensive control frameworks (supported by expensive applications)
to ensuring that they have balanced information at their disposal.

19. From focusing on preventive hard controls
to paying ample attention to the importance of competencies (judgment) and intentions (integrity).

20. From judging employees on their degrees and intelligence in appointments
to selecting individuals based on their personal values.

21. From naively referencing the marketing version of the core values on the website
to paying particular attention to real life behavior.

22. From only welcoming favorable information
to ensuring that estimates used in proposals, budgets and forecasts are based on realistic assumptions.

23. From identifying what could hamper achieving individual organizational goals
to balancing conflicting interests as best as possible.

24. From producing separate risk reports besides regular management reporting
to producing forecasts that indicate the extent to which the estimated results will fall within acceptable tolerances.

25. From expecting managers to issue (clean) internal in control statements
to emphasizing learning from positive and negative experiences.

26. From being busy with compliance requirements such as mandatory risk analyses
to being committed to sharing knowledge and best practices.

27. From approaching highly complex strategic decisions the same way as simpler challenges,
to realizing that it requires a different approach if useful models and ample historical data are lacking.

28. From going along with unfounded optimism
to being aware of wishful thinking, groupthink and a host of other common biases.

29. From thinking that they are already there when the decision has bene made
to realizing that the associated disadvantages still have to be dealt with if they choose an option because of its perceived benefits.

30. From still treating 'risk management' as a separate agenda item
to realizing that all business decisions require looking ahead and making choices under uncertainty.