Is Risk Management Redundant?

Transcript of the presentation by Marinus de Pooter at the IIA International Conference in Amsterdam on July 11, 2023

1. Is Risk Management redundant?

Recent insights in dealing with the uncertain future have major ramifications for professionals who love to talk about risks all the time. Think of: risk managers, compliance officers, privacy specialists, information security officers, safety consultants, business continuity experts, resilience people and internal auditors.

I became involved in the risk management world almost 20 years ago when I joined the Business Risk Services practice of EY Advisory. At that time COSO had issued their ERM Framework, the famous colorful cube with the 8 components. This was all pretty new and exciting. A new framework developed by one of our main competitors, PwC.

As regional ERM Solution Leader I was part of a global team that was responsible for shaping and adapting the risk management methodology to serve our clients. I made myself guilty of developing paraphernalia such as risk workshops, risk registers, risk profiles, risk indicators, risk reports and what have you. Gradually I started asking myself: "Is risk management redundant?"

What do I mean by 'risk management' and by 'redundant'? Risk management the way it's applied in many organizations, conventional risk management, is a formalized approach to deal with the uncertain future. It's aimed at identifying, analyzing, mitigating and monitoring all sorts of risks. The underlying thought is that there are loads of risks out there. And you got to do something about it.

Redundant has different meanings: that there is more than is necessary, that something is no longer necessary or not needed at all. I mean the latter. So, the question is: is risk management - as a separate system, program or function - superfluous, inessential, unnecessary?

In COSO ERM 2004 risk management was still seen as a process. As you may know COSO ERM 2017 came up with a completely different definition. Enterprise Risk Management became: the culture, capabilities and practices that organizations rely on to manage risk in creating, preserving and realizing value.

Chances are high that you believe that risk management can be implemented. Or even, that you think that it is absolutely unwise not to do so. It saves decision-makers from unnecessary pitfalls. Above all, managing your risks would help them achieve their goals.

In risk management approaches typically people zoom in on what can go wrong in the future. They then make substantial lists of risks (risk portfolio, risk register). Tim Leech and others call this "risk list management". This focus on negativity was underscored by the COSO Internal Control framework. It states that opportunities aren't part of internal control, but of management. If you happen to come across an opportunity, don't touch it! Channel it back to the objective setting process.

Great importance is attached to completeness. As a result, those risk lists are not only long, but also wide: with lots of columns in a spreadsheet. The risks identified are usually categorized

using a taxonomy. And they are prioritized - usually qualitatively - using risk scores based on risk criteria for likelihood and effect with scales ranging e.g. from 1 to 5 or 6 or whatever.

Controls, control measures, play an important role in this approach. You absolutely need them to mitigate your risks. Periodic reports with information on the "state of risk" are submitted to the management team and the Board. I bet you recognize this from your own experience as it is a very common approach.

2. What are the ramifications of redundant Risk Management?

As a thought exercise, what would be the ramifications if risk management were redundant? For example, for internal auditors? These are the people who in real life are supposed to audit risk management. We all know that internal auditors love to talk about risks. They believe that if an internal auditor has a good understanding of the applicable risks related to the audit object then the rest of the work is relatively straightforward.

Per the current international standards (#2120) the Internal Audit function must evaluate the effectiveness of the risk management processes and contribute to their improvement. This is about the auditee's identification and assessment of significant risks and their selection of risk responses. Based on yet another standard (#2010) the Chief Audit Executive must perform a risk assessment at least once a year as the basis for the risk-based internal audit plan. He or she must take into account the organization's risk management framework.

The organization's audit universe must include all major risks: the key risks. All this is to provide sufficient assurance that the significant risks have been effectively mitigated by the risk management and control systems. The underlying idea in the internal audit standards is that organizations face lots of risks and should do something about them.

There are quite a few people involved in the risk management world. How about the people who have been appointed to 'risk owner' by their Risk Management colleagues? Or executives who are a member of a Risk Committee. Some individuals are even Chief Risk Officer - the supreme risk person in their organization.

I'm not even talking about the countless risk consultants and risk management software vendors. And let's not forget all those risk managers who are busy in their organization with finetuning Risk Control Self Assessments. You probably know specialists who work on state of risk reports and on risk paragraphs in annual reports.

However, if risk management is the answer what was the question again? International standards like COSO ERM and ISO 31000 promise to create and preserve value. To which extent are these conventional risk management approaches going to help decision-makers to 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 involves competing or even conflicting interests. Imagine a producer of PFASs, synthetic chemical compounds that we all use. These man-made substances are used 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.

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 situations like this? I invite you to ask yourself whether decision-makers need something separate called 'Risk Management' if the following is already part and parcel of their daily management activities:

1. They understand that staying future-proof requires that their core stakeholders remain satisfied with their performance. Their objectives express the value that they want to create and protect for these stakeholders.
2. They anticipate, look ahead and keep an eye on what's going on in the world around them. They want to be aware of potential changes in circumstances that could impact what their core stakeholders value: positively, negatively or both.
3. They make decisions under uncertainty, balancing estimated pros and cons. They face dilemmas as their core stakeholders have competing or even conflicting interests.

Before we dig into this a bit deeper, let's have a brief look at the history of conventional risk management.

3. How did the current Risk Management practices come about?

As early as the 1960s the first requirements of the SEC, the Securities and Exchange Commission, emerged in the United States. They were about 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. All this is aimed at preventing financial losses for those involved. Who - apart from the fraudsters - doesn't appreciate shareholder protection?

In pursuit of improvement, particularly in response to spectacular failures, a variety of remedial ideas and practices emerged from diverse groups.

1. Think of those with financial interests such as insurers. With increased predictability about what might happen insurers could be more confident that their pricing would allow them to still make a decent profit after paying the claims. One of the ways to do so was to coerce their clients to adopt a myriad of practices that they called 'risk management'.
2. Governments and their regulatory agencies were (perceived to be) accountable on behalf of the public for avoiding serious accidents and disasters. From this governments and regulators were able to enact and enforce laws to constrain decision-makers in organizations. Think of safety requirements in construction and minimum liquidity requirements in banking.
3. There was a third category comprised of groups who started to focus on and publish about improvements: academics, management experts and gurus. They developed for example Total Quality Management.
4. Progressively, an important fourth group emerged: external consultants. They recognized a commercial opportunity to provide the 'how to' services. Of course, their purpose was to support organizations seeking to improve their operations. However, self-interest may have led many firms to become inventors and then advocates for their own methods.

5. 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.

In order to better understand the current practices of conventional risk management, let's have a look at the origin of the risk registers. These 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.

Those lists with points of interest in the factories were never primarily designed to achieve balanced decision-making. People are not going to consult their risk register when facing dilemmas or making tough decisions. If you come across a list of risks in annual plans, team plans and project plans, now you know where they come from.

A separate risk management function, role or department easily induces the situation that colleagues quickly think: if you have queries about risks you shouldn't ask me, but contact those specialists since they are there for you.

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. And that function must then 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.

However, you should especially ask yourself how realistic it is to think that with a herd of risk officers and compliance officers you can keep the cowboys in question on the right track. If line managers are only held accountable for and rewarded for their commercial performance, then compliance will soon be defeated.

Reconciling dilemmas is mainly about attitude and mentality. Mentality is the thinking and behavior pattern of a person or a social group. It is what they find normal. It is closely related to their core values: their beliefs and ideals about what is acceptable and unacceptable behavior. You probably also know these people who reason like this:

- "If they don't want us to do this, then they should ban it."
- "Fines from regulators are just ordinary business costs."
- "As long as we aren't caught, we aren't doing anything wrong - formally speaking."

Due to their role supervisory authorities are hardly interested in the 'upside' of risk. They are focused on avoiding trouble and misery. Many directors still 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 supervisory authorities.

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

trainings board members and supervisory directors are taught to ask about the top 10 risks. That is apparently a sign that people have thought carefully about their vulnerabilities.

Internal specialists and external consultants used risk management to help organizations limit their risks. It led to all kinds of methodologies and codifications of best practices: the internal control and risk management standards.

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, risk reporting and what have you.

The more these best practices were made mandatory, the more lucrative their revenue models 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. All major consulting firms are now jumping on this bandwagon. Risk and compliance management is a multi-billion dollar industry with huge commercial interests.

It is salient, however, that you very rarely encounter business people like entrepreneurs, directors, line managers or project leaders at risk management training courses or conferences. That's quite remarkable, because risk management promises to help them achieve their objectives better. Most of them are not retarded. If it really helped them, wouldn't they sit in the front rows and learn how to take advantage of it?

In practice, risk management has become an accountability tool. Decision-makers are expected to demonstrate how well they are able to prevent and detect things that might go wrong. Providing evidence of compliance is quite different from a tool to achieve your goals under uncertainty. This conventional risk management approach is practiced so widely. You have to ask yourself though whether it really actively helps line and project managers to make better decisions.

4. 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, “risk” has several meanings, such as:

a. an uncertain event that if it happens will have an effect on what we are trying to achieve;
b. the cause of that event, like a risk source, a risk factor or a risk driver;
c. the event itself;
d. the consequences of that event, also called impacts or effects;
e. the volatility of the expected value.

ISO is the International Organization for Standardization (IOS). Their business model is standardization. It is striking that ISO after all uses more than 40 different definitions of risk in its own documents.

The term “risk” itself is extremely confusing. In COSO IC (2013), COSO ERM (2004) and for that matter also in common parlance, 'risk' 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.

This has significant implications. Originally, COSO had four so-called risk responses: Accept, Avoid, Reduce, Share. 'Pursue' was added as the fifth risk response in 2017: "Accept increased risk to achieve improved performance." However, for the average safety consultant pursuing risk is like swearing.

This implies that simply the use of the term 'risk' is already causing problems. Despite the changes in the definition of 'risk' numerous professionals are still trained to ask what-can-go-wrong questions, to produce lists of risks and to come up with controls to mitigate them. That is by no means a holistic approach.

Think about it: when you start investing hopefully you are not only concerned with possible losses, but also with returns. When you apply 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. You also consider personal development opportunities, supportive colleagues and inspiring assignments.

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. That is no surprise as in common parlance 'risk' has a negative connotation.

Because of all this confusion people like Grant Purdy advocate avoiding "the R-word". "Uncertainty management" or "success management" are already better terms. Or take for example the term "value management". After all both COSO and ISO indicate that risk management is all about creating and protecting value.

The big advantage of referring to 'value' is that it makes you realize that terms like 'value', 'result', 'success' or 'improvement' themselves 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 physical or social safety, information security, innovation, punctuality or sustainability.

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 with all your might into the existing management cycle in order to become successful. In practice, this is not easy at all and we all know 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, the allocation of tasks, authorities and accountabilities;
- 'risk owner' in addition to someone who is in charge of achieving objectives when managing a department, function or project;
- 'risk culture' besides people's customs and behaviors in your organization.

According to many in the risk management world you have to make all kinds of statements about your risk appetite. It is one of the artifacts of conventional risk management. Risk appetite is about the types and amount of risk you're willing to take.

Risk appetite isn't a very useful concept, unless you consider both risk and reward. Do decision-makers consider risk appetite when pricing products or hiring colleagues? And 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 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 ideas about potential future events, situations, circumstances, and so on. Our images are strongly influenced by our personalities, knowledge and experience. Plus we humans suffer terribly from biases, from prejudices, from flawed thinking.

Take for example group think that is very common. Conforming to the group's dominant views saves someone a lot of hassle. One could argue that conventional risk management itself is based on the loss aversion bias. We appear to experience the pain of (possible) loss twice as much as the pleasure of (possible) gain.

COSO ERM 2017 defines 'risk' as: the possibility that events will occur and affect the achievement of strategy and business objectives. Several thought leaders indicate that it is a fundamental error to look at risks as events rather than as cause and effect relationships between what happens.

As events aren't independent we need to think about correlations. Risk assessments, particularly analyses like the BowTie, assume cause and effect relations. Many of these relations are knowable only in hindsight. Or not knowable at all, since they are way too complicated in reality.

Knowledge about cause and effect relations is captivating. The assumption that global warming is anthropogenic can be pretty useful for you. Making people terrified and feel guilty enables them to behave in a way that serves your own interests. Churches have applied these tactics for ages.

In practice many risk assessments are done qualitatively. Scores are then awarded to estimated likelihoods and effects. Using values on ordinal scales (for example, from 1 to 6). This is the same type of scales that is used in opinion polls and the number of stars to indicate the quality of hotels.

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

This is the established approach in many industries. The heavy reliance on human judgment to estimate future events constitutes a material vulnerability in the conventional approaches. And we cannot simply multiply values on ordinal scales.

Risk quantification is highly dependent on the quality and quantity of the available data and the assumed dependencies between factors. They simplify complex real-world systems and processes. If the assumptions are no longer valid, then the value of the model expires. Identifying key assumptions and checking their validity are basic steps to ask probing questions and to add value.

Statistical data from the past should be handled with care. Take for example mortality tables. We now have serious excess mortality and underbirth. Plus 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. Yes, maybe in the old 'shareholder value' way of thinking: maximizing the value for shareholders (the earnings per share). 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. Take for example the massive violations of human rights.

5. What is the essence of the new insights?

The new insights are quite different from the conventional approaches. The latter focus on risks. They assume that loads of bad things can happen. Therefore, you must have separate risk management to mitigate them. To ward off disasters, you must invest in risk identification, risk analysis, risk mitigation and risk monitoring.

Many internal auditors are familiar with the 'ORCA'- approach. If you know what you want (your objectives), cleverly think of what might go wrong (your risks), implement suitable measures (your controls) and obtain evidence that they work (your assurance) then reality will unfold itself as anticipated. This is the illusory control world. In this world unplanned success is just about the worst thing that can happen to you.

In many risk management approaches, the people responsible for achieving key business objectives are not expected to formally assess and report upwards on the level of uncertainty that the objectives will be achieved. The structured documented assessment rests with functions like Risk Management or Internal Audit.

The conventional approaches were increasingly challenged during the past years. Thought leaders indicated that the following duties are part and parcel of your regular work as a decision-maker, as an entrepreneur, director, line manager, project leader, et cetera:

1. remaining futureproof through keeping your core stakeholders satisfied by creating and protecting what they value;
2. anticipating, looking ahead and analyzing the potential effects of what can happen on the interests of your stakeholders;
3. making tough choices consequent consciously when reconciling dilemmas.

Decision-makers have to estimate and weigh the potential pros and cons. Rarely does anything in life come with benefits only. There are always drawbacks, too. If you hire someone because of his or her desired properties, you also have to cope with their unpleasant personality traits.

Balanced decision-making requires that you consider both potential positive and negative consequences. If you choose for an option because of the perceived advantages, you still need to deal with the associated disadvantages. What are necessary buffers, reserves, plans-B that you may need?

Take, for example, buying a home. Obviously, home ownership comes with significant advantages such as capital accumulation and more freedom to adjust your house to your personal taste. There are also serious possible disadvantages particularly in case of a mortgage. That's speculating with borrowed money. Or subsidence of the foundations due to changed groundwater levels.

Same with capacity. Please realize that it doesn't make a lot of sense to ask what are the potential negative consequences of overcapacity or of undercapacity. Less return on your assets and having to say 'no' to your clients. Both have potential positive effects as well. Overcapacity means that you can easily serve a new client. And your undercapacity could imply scarcity in the industry justifying higher rates.

Always focus on the interests when weighing pros and cons! Don't forget that many people earn their living based on preventing and handling adversities. Think of doctors or people repairing your cars and laptops.

As a management team, you will not become successful by combating misery and limiting failures. You become successful by seizing opportunities that help you to perform better than expected. And by limiting serious 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 your dilemmas. It all comes down to making decisions and therefore it is all about regular management. Day to day management relates allocating scarce people and resources through policies, processes and procedures in order to deliver products and services that meet requirements and expectations.

Allocating people and resources in order to benefit from an opportunity or to mitigate a threat comes with an opportunity cost: they can't be invested in other initiatives. So, you have to choose. Decision-making is not just about information and knowing how to apply it. Decision-making is primarily about mentality.

As a decision-maker are you are responsible for dealing with competing interests. You have to weigh possible pros and cons associated with your different options. Decision-making only becomes interesting in case of dilemmas. Then you have to choose.

Remember the situation you were in as a citizen during the last few years. Your government were promoting with all marketing forces available that everyone gets injected multiple times. They assured you that the solutions were safe and effective. If you didn't comply, your access to society was restricted. However, the vendors didn't accept any liability. You weren't updated on the adverse effects occurring. Scientists who challenged the safety and effectiveness claims were censored. Anyone who dared to doubt the official narrative was deplatformed on social media. This wasn't an easy choice to be made for many people.

Weighing the possible advantages and disadvantages is quite different from having a separate risk management initiative, system or even function. It is all about dealing with the uncertainty that your objectives will be achieved. Are they achievable anyway? Are you aware of your main dependencies?

In order to be able to manage the expectations of your core stakeholders you need to be able to report on the likelihood of your success, of your performance. Estimating and weighing pros and cons is quite different from maintaining lists of risks and reporting on them in a State of Risk report.

It doesn't make sense to spend endless time identifying risks and measuring risk levels. Labelling something as "high risk" doesn't necessarily help those who have to make tough decisions. A high risk can still be acceptable if it comes with high potential returns.

6. What can we learn from the new insights?

We have reviewed the development of conventional separate risk management. The focus is on risk control: individual risks should be kept at acceptable levels. It turns out that the conventional approaches mainly serve compliance purposes. They easily degenerate into an illusory system.

Inherent in the regular management responsibilities is the focus on:

1. staying future-proof through keeping your core stakeholders satisfied;
2. looking ahead and analyzing what can happen that affects their interests;
3. making your decisions consequence consciously.

Decision-makers can very well use the help of critical friends when anticipating the uncertain future. In other words, they need knowledgeable colleagues who keep them on your toes as their coach: decision support. The critical friends help them increase the likelihood of their success. They help them with making realistic plans, scenarios and forecasts, balancing pros and cons and reconciling their dilemmas. They do so through making them aware of their own biases, ensuring the right experts are involved and providing reliable information about what might happen.

Critical friends make them aware of marketing tricks, too. Marketing is an ingenious profession with sophisticated influencing techniques. Decision-makers should always be on guard that there are people who want to mark the advantages and mask the disadvantages. Take for example the 17 Sustainable Development Goals. If one doesn't not know a lot about the origins of Agenda 21, Agenda 2030 and the New World Order these SDGs sound like an fantastic 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 technocracy. This movement emerged after the disastrous effects of the choices of the politicians: the Great Depression. A group of scientists, engineers and bureaucrats concluded that allocating the world's resources should better be left to experts like themselves who know how to use models.

Thinking about it achieving these SDGs will only be feasible by implementing extensive digital surveillance. It requires a structure whereby your countries' governments act as the middle management of corporate states like BigTech companies, of huge investment funds, and of powerful NGOs.

Here are some key take-aways for internal auditors who want to go beyond reporting internal control deficiencies:

1. Understand that organizations are future-proof when they are able to keep their core stakeholders satisfied. Different stakeholders value different things. So, decision-makers have to choose.
   Do the decision-makers have the competence, integrity and commitment to reconcile dilemmas?
2. Understand that success is dependent on the quality of the decision-making under uncertainty. It includes both strategy setting and realization. So, it is not about managing individual risks, but about dealing with competing interests.
   Do the decision-makers use a structured balanced approach for making their choices and reconciling dilemmas?

3. Understand that being consequence conscious implies: weighing the potential pros and cons whenever important decisions are to be made.
   Are the decision-makers reminded of wishful thinking and numerous other biases?
4. Understand that decision-making has everything to do with integrity, morality and mentality. Integrity means sticking to your norms and values even if under pressure and seduction.
   Are the personal values of the executives assessed before hiring them?
5. Understand that it's crucial to investigate which interests are dominant. If only short term commercial goals predominate, then that is a huge red flag.
   Which core values do you find, not when you look at the auditee's website, but when you look at the actual mentality and behavior of the executives?
6. Understand the limited value of updating risk lists and making risk analyses. It's not about managing isolated risks individually.
   Does the auditee still produce heatmaps? Nobody uses them whenever important decisions have to be made. Talking about risk levels doesn't make a lot of sense. For proper decision-making decision-makers have to balance pros and cons.
7. Understand that questions like what-can-happen? and what-if? are essential. They need to be asked at all levels when dealing with the uncertain future.
   Are assumptions in plans challenged and are multiple scenarios used?
8. Understand that decision-makers need to be kept realistic of possible consequences of their choices to act or to refrain from acting.
   Do the decision-makers see the big picture, appreciate that unwelcome information is brought forward and support colleagues who have the courage to speak up?
9. Understand that using risk management jargon makes ordinary people think: this must be different from my daily work as it is stuff for risk experts.
   Does the auditee use the language of the business when dealing with uncertainty?
10. Understand that there is every reason to remain modest. Our human abilities to understand the future are really limited.
    Does the decision-makers realize that the actual results are always a combination of luck and misfortune on the one hand and wisdom and unwisdom on the other hand?

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 of the implications of artificial intelligence, quantum computing or the internet of bodies (transhumanism).

Regardless of the industry effectively managing the business under uncertainty requires:

- competent, honest and committed decision-makers;
- people who are alert to what is going on;
- a culture in which the bringers of unpleasant news are appreciated;
- the ability to improvise.

If your auditee has to deal with a supervisory authority who still believes in risk management paraphernalia, then advise them to start a conversation about the new insights. If that doesn't help, they should try their best to meet the basic compliance requirements. But spend as little capacity on it as possible. Instead, use their time, energy and attention to help their colleagues

make balanced decisions.

Marinus de Pooter is an independent interim professional, consultant and trainer. He focuses on supporting leadership teams in remaining future-proof through 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.