NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

menu

Home › Magazine

Opinie: Is Risk Management redundant?

17 januari, 2024

Opiniestuk Marinus de Pooter

Marinus shares recent developments with significant implications for internal auditors in this article.

An inconvenient yet intriguing question

For many risk, compliance and audit professionals simply posing the question will immediately raise their eyebrows. For them managing risks belongs to their profession as fireworks belong to New Year's Eve. However, in recent years the understanding of dealing with the uncertain future has changed considerably. In this article I share recent developments with significant implications for internal auditors.

Risk management can and should be implemented according to many experts. They believe it is profoundly unwise not to do so. It saves you from unnecessary pitfalls and above all risk management helps you achieve your goals. How on earth could it be redundant?

Organizational leadership has to do something with risks. This is the underlying principle in the international risk and audit management standards. The internal audit function is supposed to evaluate the effectiveness of the risk management processes and contribute to improving them.

Many people have been assigned roles in the risk management world. Think of those who have been designated as 'risk owner' by their Risk Management colleagues. Countless individuals make their living as internal risk managers, risk officers or risk analysts. Not to mention the numerous external risk advisors and software vendors.

Risk consultants keep selling and many organizations continue to buy risk frameworks, risk assessments, risk registers, risk matrices and risk dashboards. All these tools are designed to capture, analyze and deal with individual risks or separate risk categories.

Tim Leech and others refer to this approach as 'risk list management'. The underlying belief is that the ultimate goal is the mitigation of what can go wrong. However, as

Alexei Sidorenko points out e.g. in his book 'Guide to effective risk management 3.0', it is not managing risks but about making better decisions.

If risk management is the answer, what was the question again? How well do the conventional approaches 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 serious commercial interests in maintaining this system?

To which extent do decision-makers need something separate called 'risk management' if the following applies?

1. They understand that staying future-proof requires that the core stakeholders remain satisfied with their performance. Their objectives express the value that they need to create and protect for these stakeholders.
2. They look ahead, keep an eye on what is going on in the world around them and anticipate. They focus on potential changes in circumstances that could impact what their core stakeholders value - positively, negatively or both.
3. They are aware of uncertainty when making decisions. They display a mentality that leads to balanced choices and honest reconciliations of dilemmas.

Serious issues with conventional risk management

Recent insights underscore multiple issues with common risk management approaches. Roger Estall and Grant Purdy conclude in their book 'Deciding' that risk management is a millstone hanging around the neck of organizations that should be abandoned.

First of all, what are we talking about when using the word 'risk'? Unfortunately, there

is no universal definition. The business model of ISO is standardization. It is striking that they use more than 40 different definitions of risk in their own documents.

In COSO IC (2013), COSO ERM (2004) and for that matter also in common parlance 'risk' refers to something negative. Something that can cost you money, be bad for your health or discredit you. On the other hand, the ISO 31000 Risk Management Guidelines (from the start in 2009) and COSO ERM (2017) use a neutral risk concept. It concerns both positive and negative effects on the achievement of objectives.

This change comes with far-reaching consequences. Originally, COSO used four so-called risk responses: Accept, Avoid, Reduce and Share. COSO added Pursue as an extra option in 2017: ‘accept increased risk to achieve improved performance.’ It is more in line with the common concept of balancing risk and return.

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 by no means holistic. When you start investing, you are not only concerned with possible losses, but also with potential returns. Success is dependent on both benefitting from opportunities and reducing threats. Alternatively, if you use the neutral definition, implying both upside and downside risk, you lose most people in your audience right away. For them 'risk' has a negative connotation.

Because of this confusion several thoughtleaders suggest avoiding the ‘R-word’. ‘Uncertainty management’, ‘success management’ or ‘expectation management’ are already better terms. The same goes for ‘value management’. After all both COSO and ISO indicate that the purpose of risk management is creating and protecting value. It also takes into consideration that different stakeholders value different things, such as safety, financial return and punctuality.

One of the artifacts of conventional risk management is the ‘risk appetite statement’. It

refers to the types and amount of risk that organizations are willing to take. However, how do you express the ‘amount of risk’? There is no unit of measure for risk. With risk profiles it is suggested that you can aggregate different risks for convenience purposes. If you try to do so based on monetary value, you will soon discover that what you value most in your life is difficult to monetize.

There is no 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. Unfortunately, the chance of encountering success stories is pretty small.

What we may not always realize is 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. Above all, we humans suffer terribly from biases as Daniel Kahneman and others have pointed out.

Assessing risks is often done qualitatively in practice. Scores are awarded to estimated likelihoods and effects using values on ordinal scales (for example, from 1 to 5). This type of scales is applied in opinion polls and to rate the quality of hotels using stars. One cannot simply multiply ordinal values in order to come up with ‘risk ratings’.

Risk quantification is highly dependent on the quantity and quality of the available data and the assumed parameters in the model. If the assumptions used are no longer valid, the value of the model expires. Moreover, they remain just models; a map is not the area that it represents.

Many executives see risk management primarily as a compliance matter. To them effective risk management means above all that they don't get into trouble with their

external or internal supervisors. Due to their role, supervisory authorities are hardly interested in the 'upside' of risk. It is their duty to minimize the downside.

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

During training, Board members are taught to ask about the top ten risks. That is apparently a sign that management has thought carefully about the organization’s vulnerabilities as the basis for taking suitable actions to mitigate them.

It is remarkable, however, that one very rarely encounters entrepreneurs, line managers or project leaders at risk management training courses, webinars and conferences. This is quite striking as standards promise that risk management enables them to better achieve their objectives. Most of these individuals are not stupid. If it really would help them, wouldn't they all sit in the front rows eager to learn how to take advantage of it?

Reality is that risk management has become an accountability tool. That is quite different from a tool for trying to achieve your goals under uncertainty. To which extent do the usual risk management practices really help decision-makers deal with their dilemmas?

The origins of conventional risk management practices

As early as the 1960s the first requirements of the Securities and Exchange

Commission emerged for the inclusion of risk factors in documents in the context of Initial Public Offerings. In 2005 there were requirements to include them in annual and quarterly reports. This concerns factors that make shares speculative for shareholders. It turned into the requirement to have a Risk Management Framework: a coherent set of risk identification, analysis, mitigation and monitoring. All aimed at preventing financial losses for those involved.

Internal specialists and outside consultants used risk assessments and treatments to help organizations limit undesirable outcomes. It led to methodologies and codifications of best practices. In the 2004 edition of the COSO ERM Framework risk management was seen as a process. If you had not implemented it yet, the consulting firms were lining up to assist you.

Extensive maturity models resulted in more bells and whistles. Numerous special ERM, GRC and ESG applications have been developed. The more the risk management practices became mandatory, the more lucrative the revenue models became for the advisors. It's now a multi-million dollar industry with big stakes.

In the financial sector, legislators and regulators came up with a risk management function that must even be independent of management. This function has a sheriff type role with the purpose of keeping certain cowboys on the right track. It must inform the Board based on its own risk assessments.

Over the years risk management became treated as a separate, standalone or even independent process and function. COSO made the wrong turn by explicitly excluding opportunities from internal control. Due to the maniacal focus on what can go wrong less attention was paid to the real purpose of dealing with uncertainty: helping decision-makers with identifying and weighing pros and cons when faced with dilemmas.

The idea of makeability is rampant in the planning & control world. Risk management naturally fits in well with this DNA. It can be summarized by the

ORCA-approach: stating your Objectives, identifying your Risks, implementing suitable Controls and obtaining Assurance through monitoring their effectiveness. Its promise is that it will increase the likelihood that the future is going to unfold itself as anticipated.

In order to understand the current risk management practices we also need to go back to the origin of the risk registers as the basis for the common 'heatmaps'. The risk inventory lists became common in factories in the 1970s. There they had started using lists with all kinds of points of attention regarding the safety of the workers.

When more and more regulations came 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.

Governments and regulators subsequently embraced these working standards as methods for demonstrating that organizations have their affairs in order. '"Doing risk management"' (read: keeping risk lists) was gradually seen as a characteristic of good organizational governance.

The essence of the recent insights

According to the conventional approaches it is smart to implement something separate called 'risk management' aimed at countering identified potential troubles. In order to become effective, its paraphernalia need to be integrated in the existing management system.

Recent insights start from the perspective of the decision-makers. They should not

focus on managing risks, but on managing the expectations of their core stakeholders. The aim is to help them look ahead in a consequence-conscious way, thereby considering the potential effects of acting or refraining from action on the interests of their core stakeholders. These activities are part and parcel of their daily business responsibilities.

As a decision-maker you have to weigh the estimated pros and cons of your various options to act and to refrain from action. There is nothing in life that comes with benefits only. There are always potential or actual drawbacks, too. Take for example buying a home. Homeownership does not only come with advantages, such as capital accumulation, more freedom to adjust it to your own taste and lower monthly costs than renting.

It is essential to consider the possible disadvantages as well. In essence, if you have a mortgage loan you are speculating with borrowed money. You may also end up in the unlucky circumstances of having to deal with subsiding foundations or annoying neighbors.

Management is about making choices when allocating scarce people and resources in order to deliver products and services that meet requirements and expectations. Unilateral focus on combating misery and limiting failures will not make a management team effective. Success requires both seizing opportunities and limiting threats.

Periodically updating a list of things that could 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 e.g. in his book ‘Risk Management in Plain English: A Guide for Executives’. It is not about managing individual risks, but about dealing with conflicting interests and about reconciling dilemmas.

Balanced decision-making requires factoring in unwelcome information as well. Marketing is an ingenious profession with powerful influencing and framing techniques. As a decision-maker you should always be aware of people marking the advantages and masking the disadvantages. Hence the importance of ‘critical friends’ supporting your decision-making. Individuals who keep you on your toes, remind you of your biases and challenge the assumptions in your plans and forecasts.

It remains remarkable that many people still believe that there is value in updating risk inventories for the sake of identifying risks. The same goes for spending endless time on assessing ‘risk levels’. Instead of focusing on the ‘risk status’ people should care about increasing the chance of performing as required.

Separate risk management easily degenerates into an illusory compliance-driven system. What executives really need to know is the likelihood of meeting the expectations. Why would they first create a separate risk management system and then try to integrate it into their existing management system? It is much wiser to start from the perspective of the decision-makers.

Finally, there is every reason for modesty. Our human abilities to predict the future are seriously limited. It is never possible to imagine in advance what could happen in a world with so many actors and factors. That is a complete illusion. Hence, the need for developing the improvisation skills of teams. Last but not least, we shouldn’t forget that in hindsight (un)favorable results are always a combination of (un)wisdom and (un)luck.

Key take-aways for internal auditors

1. Organizations remain future-proof when they are able to keep their core

stakeholders satisfied. Different stakeholders value different things. Hence, the executives have to choose.
Do the auditee's decision-makers have the competence, authority and resources to deal with conflicting interests?

2. Making choices and balancing interests has everything to do with ethics and integrity.
   Are the personal values of the executives assessed when hiring or appointing them?

3. It is crucial to investigate which interests are dominant. It is a huge red flag if only short term commercial goals predominate.
   Which core values do you find, not when looking at the auditee's website, but when observing the mentality and behavior of the executives?

4. Both strategy setting and realization require making choices. The quality of decision-making under uncertainty affects the likelihood of success of an entity.
   Do the decision-makers use a structured and sound approach for making impactful decisions and for reconciling their dilemmas?

5. Executives need to see the big picture and they must be kept realistic of possible consequences of their choices to act or to refrain from acting.
   Are the decision-makers aware of and reminded of wishful thinking, groupthink and numerous other common biases?

6. Updating risk lists and performing risk analyses is of limited value. It is not about managing individual risks. Talking about risk levels does not make a lot of sense if the returns are not considered, too.
   Does the auditee still use risk registers and 'heatmaps' that nobody uses when important decisions have to be made?

7. Questions like 'what-can-happen?' and 'what-if?' are essential. They need to be asked at all levels when making decisions.

Do the executives analyze the potential consequences of what might happen for their core stakeholders?

8. The right experts need to be involved in the decision-making process. Adverse information must be welcomed in order to ensure that the estimates used in proposals, budgets and forecasts are based on realistic assumptions.
   If the executives decide to go for an option because of the perceived advantages, are they reminded that they still have to deal with the associated disadvantages?

9. Using risk management jargon makes ordinary people think: this must be stuff for risk experts as it seems to be so different from my daily work.
   Does the auditee use business language when dealing with uncertainty?

10. All business decisions are about looking ahead, about balancing potential pros and cons and about making choices under uncertainty.
    Is ‘Risk Management’ still a separate item on the auditee’s meeting agendas?

About the author

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 website and LinkedIn profile for further details.

Laatste nieuws