avedos GRC Podcast

episode 9 (part 2) | GRC strategy, training of employees & simulation methods

with Michael Rasmussen (internationally recognized pundit on governance, risk management, and compliance, hereinafter referred to as **MR**) and Samuel Brandstätter (CEO & Founder of avedos GRC GmbH, hereinafter referred to as **SB**).

Vienna, December 22nd, 2020

Disclaimer

The content contained in this document is for informational purposes only. All content herein has been created with great care and to the author's best knowledge. There is no guarantee for the currency, completeness or correctness of the content on all pages. Forward-looking statements are assumptions and, therefore, no guarantee.

The content and images published in this document are subject to copyright laws. Any replication, modification, distribution and evaluation in any form beyond the copyright limitations requires the previous written consent of the respective copyright owner or author.

Version 3, 2020

SB: I think this connectiveness of risk and other GRC information related to risk is a very important topic. In the case of COVID 19, a lot of managers are asking about the consequences if we are running into a second lockdown. What happens to our risk bearing capacity? What are the benefits of an integrated GRC strategy?

MR: Companies must see this interconnective nature of risk and its impact on performance. Risk management deals with uncertainty. Companies have different objectives. For example, there are division or department objectives, process, or product objectives. It is important to map the risks to those objectives and to understand this interconnectedness.

SB: Objectives are very frequently changing in organizations. Also, if the strategy keeps in place, the way of tackling this strategy changes. Each change of this strategy has an impact on my risk portfolio. This leads to this interconnectedness. What are some of the roadblocks, issues, and hurdles for developing and implementing an integrated GRC strategy?

MR: The roadblocks I often see right now is a clear value proposition – a business case. In case of COVID 19 there is a lot of interest in improving GRC and risk management strategies. But it's not like an open checkbook. You must clearly articulate what's the value in business case or moving forward with this strategy in this solution. You need so built a strategy that defines how to make it more efficient, effective, and agile.

SB: We have seen it with one of our customers in Switzerland. It was a very interesting project where the board of directors with the owners of the company have created some kind of simplified communication instrument, which was a barometer where you have the risk bearing capacity of the company based on the financial figures. Then the management got an acceptance level to decide what risk can be taken. They could analyze what operational risk has to be taken to tackle to projects and new markets. That was the turning point where the management understood what does risk management on the operational and on the strategic level brings as a benefit. Do you also see it in the same way, that it is an instrument to discuss how to allocate my risk bearing capacity? Is this often used in companies to get to this benefit view on risk management?

MR That is a very mature risk function to deliver that. Too often risk management seems like a compliance exercise and is not part of the company culture itself.

SB: That's also our experience in the market. One of the requirements that we often see is, to use quantitative methods and in some case also risk simulation. Many people fear that this is too mathematical, very complex and hard to understand. What do you think about this topic? In Germany the IPW PS 340, which is a auditing standard for risk management from the auditing companies, is very important. Quantifying risk and taking this risk capacity related to the risk portfolio is a real legal requirement. Do you think that brings a benefit into this discussion?

MR: It will. Some companies just use it like an exercise and don't see the value and to achieve the purpose that it brings.

SB: Could that also be a training and education topic? Many of our customers start thinking about these quantitative methods, simulations, aggregation of risks. Is it also some limitation you see here regarding the education and information of employees about these quantitative methods?

MR: There is a lot of education that must take place there. We need to make sure that not only the second- and third-line functions understand those quantitate methods. We must present it to the front lines, the operational management, that owns that risks. They must understand these methods to take actions. The training and awareness of the front lines is very important.

SB: What we see is that in a lot of cases this training aspect has multiple dimensions. One is the methods side on training. Regarding GRC technology we also see that often the training of people, to participate in the processes in a risk management or GRC Software, is a pain to customers because they have frequently changing user. Do you think that this is somehow a limitation on engaging the first line? Because you said it is part of being agile in GRC to involve an engage the first line to take part in this process. Is training something that needs to be tackled to improve the actions in the past?

MR: Definitely! You need to train people about the technology. You must provide the necessary information. And it is also important to train people about the risk management culture in the organization.

SB: What are the ways to change risk culture in your sense? Is there some type of a cookbook of how to tackle the thinking model of risk management in people's heads?

MR: In my opinion that starts with awareness that risk is owned by the business in the front lines. Too often I think the employees' concept is that the chief risk officer is responsible for risk. To me a chief risk officer is more of a facilitator and collaborator. They must monitor the risk and see the interconnections of risk. The key to change risk culture in a company is developing a clear understanding, that risk is owned by the line of business.

SB: That's interesting because I think that's a thing where software really can help. What we have seen in a project is a funny episode in some way. One of our customers was doing risk management with assessments from the second line with a few people in the first line. The few people in the first line were thinking: "Ok, once a year the risk manager is coming to my office, asking me something about risks, and then he goes away with his risks." I am absolutely with you that this culture change needs to be in their heads. What we also see is, that this culture change also needs to be done for quantitative methods in risk management. In a lot of companies, we see that this risk simulation is only done by the central second line function people that are knowing what they are doing with statistics and mathematics. But it is nothing that can be done in a way to bring out to the first line managers that also need some overview on their risk portfolio. Are there some suggestions you would give to our audience of how to train people in the first line regarding those quantitative methods?

MR: It must be good communication and a step-to-step approach understanding of what it means and how to interpret and apply it to the business context. It has to be a clear communication and should not be overwhelming. People must understand how their role in the company has to deal with risk quantification and to apply it to the specific business area.

SB: What we see is that the quantification topic is something that needs good guidance. That's the reason for us to implement it to our GRC software risk2value. We offer guided tours that guide you to the whole risk management process on the one hand but also through several steps like the quantification process and really explains what is needed on the method side and on the tool perspective to run through this process. What we have seen is that this guidance really is an easy option to participate more easily without being in a 5-hour online training process. I think that could be a good way to tackle this and to gain knowledge in the first line how is their participation to their risk management process. What do you think are the biggest advantages of using quantitative methods and risk simulation compared to the "compliance approach" you mentioned and the simple heat-map view on risk?

MR: The last approaches you mentioned are failing to put a number in value on the impact of the organization. The more mature risk quantification method gives us a clear understanding of the financial impact that the business is going to bear with that risk.

SB: We need to relate risk management to performance. That means the numbers that a company produces. Because that is what the managers are accountable for. They are interested in how the risk they are taking impacts this numbers.

It was a very interesting run-through with a lot of views on GRC and to how improve risk management. I have one last question: What advice would you give to companies when developing GRC processes?

MR: You need to understand your current state – the fundamental reality. Where are we today? How are we managing risk today in the organization? What is working? What is not working? How fragmented or integrated is our risk management? Once you have understood your current state you can define your future state. You are not getting that overnight. I like 3-years-plans. What do we want risk management to look like in 3 years? How will it change from the current state? And then you must develop a project plan which defines how to get there. The project plan should also understand that you do not get there overnight. I often use that example of climbing the Mount-Everest. If you climb the mountain too fast you will die. You must go to the first base camp an let your body acclimate before you are ready to hit the next stage. It's the same thing with a big risk management project. You must tackle in stages. If you change too much too quickly the project will fail. You need a strategic plan. The other important thing is to keep the right people involved on the strategy. That helps that the risk management process will be a success. And finally, you must pick the right technology. Too often I see people that have a good vision for risk management and stick to a 3-years plan. But they choose a GRC platform that is only good in one domaine of risk. You must analyse your solution to really stick to your 3-years plan. You have to select a technology that accomplish where you want to get through.

SB: That's a very good point and a request to us as a software vendor. We need to enable organizations to take this journey step by step. That means that a software platform supporting this process needs to be easily adoptable – which means agile. It must start simple – at the maturity level of the company now – pick it up and go from that and expand and improve to a higher maturity along with this 3-years plan. That's what we as a software vendor need to support and what we want to support. We need to start where we are right now and improve step by step.

Michael it was a great pleasure to talk with you through these different topics and I think there are a lot things to dive deep into. Thanks for taking you time – especially on your birthday. Thanks to the audience for listening to this podcast episode. Keep up for the next episode of the avedos GRC podcast. Thank you very much and have a nice day.

All information about our podcast can be found on our website at https://avedos.com/ressourcen/.