Interview of Marcelo Baêta Chaves with Julia Graham on Nov. 13th, 2015 in Rio de Janeiro, Brazil:

Julia, could you introduce yourself, please?

I'm Julia Graham, deputy CEO and technical director for Airmic, which is the United Kingdom Association for Insurance and Risk Management professionals.

In your opinion, is the creation of a division to implement risk management in an organization recommended?

I think there's enough research out in the world now to show that well risk managed businesses are better managed businesses; and there's a lot of evidence from United States, from Europe and from Asia Pacific, that can now point towards the fact that well risk managed businesses generate more profit; and the more mature the risk management is, the more likely this is to be reflected in profit.

This is supported by research conducted by other risk trade associations like RIMS, the Risk Management Society in the United States and FERMA, the Federation of European Risk Management Associations in Europe (of which Airmic is member), and consultants like EY.

Which kind of training do you recommend in order to implement risk management in an organization?

That's a very big question, so think that I'll give you a very big answer. Training has to be all levels. For risk management to be successful, you have to set the tone at the top of the business, but you also have to set the tone all the way through the business; right through to the people who face customers, at the front end of the business - they all are risk managers - and therefore this is relevant to them. The key word is relevant. Everyone should have relevant training in risk management. By relevant, I mean that training should reflect whether people have responsibility for other people, special projects, country, sector or a team. Training also applies to the top of the organization. The board needs training in order to help them discharge their risk management and reporting responsibilities, because the board is ultimately responsible for managing risk in any organization.

Is it important to have a risk manager, who is part of the company to implement risk management in the company?

There should be a 'risk management champion' at the board level, who is recognized at this level as a risk 'owner', somebody openly endorsed by the chairman of the board and somebody who the chairman can turn to and say, "please, give me an update on how well we are doing?" I think you also need people who have specific knowledge and competencies in various key strategic subjects, for example digital risk, the board can turn to.

Whether you need risk management as a centralized function, or whether you need people who have risk management responsibilities and competencies embedded throughout the business depends on the business model, culture and risk maturity of the business.

Once you have a policy, a framework and you are going to start the process; do you think a pilot-project is recommended?

I think with any new processes, to have a pilot is probably a good idea. This is one way where ISO 31000 is so helpful, because it gives you a simple set of principles, a simple framework and a simple process around which you can build your own response and help to explain that response. Picking one business unit or one country in which to run a pilot is not a bad idea.

Are the techniques of ISO 31010 indispensables to do risk assessment?

I think the basic process of risk assessment is indispensable; the degree of science into which you go really depends on the business that you are in and the stage of risk management you are at. So, for example, before I joined Airmic, for eleven years, I was the Chief Risk Officer for a Global Law Firm. I didn't really use a lot of the techniques in ISO 31010 in a law firm, but I did use ISO 31000, as the foundation on which I built the law firm's enterprise risk management approach. As a benefit this often helped us to relate to clients who also used ISO language. I am a big supporter of standards, designing and embedding them as part of the firm's approach across the whole firm. ISO 31000, if you use it and apply it appropriately to a business is a great tool to have. 31010 in law has less relevance, but in other sectors can have much more relevance.

Do you think that is the analysis of inherent risk essential?

It depends, but no, I don't, personally. In some business today it is much less common to be too worried about inherent risk (even in Financial Services). And I think, again, it's like any approach to any business discipline, you have to take the basics and apply them in a way that suits your business. And what you always have to have is an explanation of why you've done what you've done, so that you have a rationale for it.

Is risk management software essential to do risk assessment?

Risk management software increasingly has a place in the risk managers' toolkit, and I used software in the law firm (and although the software was quite different, I also used it in my previous risk management role for a global insurance company). Software can facilitate consistency, provide an effective and efficient way to gather information in a way which is then consistent with how you might wish to analyze it and design reports. Data is easier to aggregate, especially if you are a global business, as my business was. You can embed a common language and whilst you might manage the software centrally and using a common system and language, you can get individual businesses that would otherwise use their own metrics, and their own language, to conform. This can help to facilitate drilling through to a local business or country view.

Most good software also includes diarized reminders and 'nag ware' which can be overseen centrally. This can be especially helpful for controls management – in my experience most people love doing risk assessments, people are much less inclined to undertake then follow through controls assessment. Software can support and report that process – including cost benefit analysis.

What guidance could you give about establishing a matrix of risks? How to establish an impact and a probability column or line in this matrix?

I would suggest that the metrics that you use have to be relevant. For example in the law firm I tied metrics to subjects partners and employees in the firm identified with. The typical law firm business model is low in capital and consequently this drives a tendency towards a low risk appetite, because you're not able to call on the capital of the firm in the event of a problem – unplanned or uncovered calls for capital will come from borrowings or even the partners' personal assets. This makes partners risk sensitive. What people in the firm readily identify with are claims from clients for malpractice. This in turn emphasizes the importance of malpractice insurance which is readily available in the commercial insurance market and the larger law firms will buy material insurance programs to protect their assets. Using the cost of risk financing, this risk is a great metric – quantifiable and relevant. To create a 'killer risk' matrix you can talk to people about where they feel a catastrophe might kill the business, outside the limit (or cover) of your insurance. You can use this discussion to explain why you approach insurance in this way, why you buy the limits and cover that you do – relating risk to their world and the potential outcome of their actions. The other thing I always did was talk about risk in language people understood – avoiding risk jargon.

Make sure you've got the right people involved in risk assessment. Information technology and information risk is a really good example. It's not just the IT manager's role to understand and manage these risks - , it's an enterprise-wide issue and a team responsibility.

And then the other thing I did because risk is becoming more intangible, when I put the risk register together, I included two extra columns in the system and software which ask whether insurance can be used as a risk control and whether the risk requires consideration of the firm's crisis management response. This is because there is a tendency to over-rely on insurance and to consider crisis management as a control for tangible asset events e.g. fires and floods. This is a great way to raise board awareness and interest – the biggest crisis they might face is most likely to involve potential damage to reputation – one of the biggest killers of professional partnership businesses. So, for every risk at a strategic level, the firm identified those which might require crisis management or as we called it a 'rapid response'. It was also interesting to see the dynamics of these risks and their controls – insurability changes over time and using the technology example, insurance cover available now is much wider and cost effective than was the case a few years ago. Similarly in a fast changing world, the need for effective crisis management has increased. This keeps the board aware that if you have a problem whilst insurance can help this is not the only risk control solution. So, it's about relating risk to the way they run their business. It's all about relevance, it's all about them identifying the issues, so that you don't appear in risk management to be operating in a risk vacuum or silo.

How to compare the importance of different risks of different areas of an organization?

I'm not sure I know how to answer that question, can you just expand for me what you're trying to get at.

When an organization has a comprehensive understanding of its risks, which risks should the organization decide to treat? How to compare…

You can't treat everything. So, I think what you have to look at are the risks that are most material to the pursuit of objectives, which is what we've been talking about this week, and to prioritize them. So, I think at a strategic level, the best way to do that is that you have access to the board on a regular basis to discuss these issues. My personal view is that a list of risks considered by a board at a strategic level should not be more than twelve or fifteen at most. Many more and they lose their relevance. Every risk should have at least one board 'owner'. Somebody, who, at the board level, says "I'm the champion, for this subject". And that champion is then charged to understand how that risk is being managed right through the business into the operational level. So, at a strategic level, risk ownership is absolutely key. And at a more operational level, making sure that people understand the importance of risk is important and that all have an ability to speak up and say if they think something is wrong or going wrong. This is why building a risk culture is so important – it should be OK to say, "you know, this doesn't look right". The one time that something looks wrong – for example on an oil rig – is the one time that something might explode and cause a catastrophe. People have to feel that they can speak up without being condemned.

To escalate, right?

Yes.

Two more questions…What are your impressions about how organizations can better take account of uncertainty? Take account or consider uncertainty, as you were talking "both when decisions are made and latter circumstances inside or outside the organization that are relevant to the decisions have changed".

I'm a great believer that organizations need to be better at scenario management. And I don't think organizations do enough of this, they try to base the future on the understanding of the past. And I think this is one area where risk managers need to grow new skills. And with the colleagues guide the organization looking into the future, asking "What if this happens? What if that happens?" I often use the expression 'meerkat risk management' – these desert animals are famous for standing up on their hind legs to look out for what going on and signs of danger. I think the risk managers are the 'meerkats' of the organization. To help businesses we've got to be a lot better at using these skills and to encourage our boards to spend more time thinking and talking and looking at the future rather than looking over their shoulders about things they already understand.

And the last one, on the design specification comment, it says "the main objective of an organization is not to effectively manage risk, to have effective controls, but to ensure to make the best decisions and achieve the objectives". What comments would you give about this?

Risk management should be a business tool. It should be something that supports the business. It shouldn't be separate to the business. And I believe that to be successful risk management needs to embedded in the business model of any organization and to be part of the way that the business does things. Whether you chose to have risk management as a separate function or whether you chose to distribute the function across the organization, I don't think matters. What matters is a common language and a common system, so that when you talk about things people understand what you mean; and you need to have access to the people and ownership by the board. Ah, but is part of good business.

All right, thank you very much.

My pleasure.