**My Dream Head of Risk and Compliance Profile** February 2018

So now, in the mix of the recruitment process we have, we have quite a good number of candidates. I'd like to share some of my thoughts on what would be, for me, the ideal Head of Risk and Compliance (RC).

So, the first major point is for the candidate to have a good vision for how risk and compliance can be an enabler for the business, something that makes the business grow faster. And basically, simplifies processes. Fundamentally, managing risks and their mitigation is a core operational practice. It's the ability to execute rules, related to regulations, very effectively and very professionally.   I'm a very big believer in a strong approach machine, which is basically an efficient process driven workflow. So, if you look for example, risk management is the ability to understand what are the implications of the decisions that are being made and allow the owners, the business owners of the assets that we are talking about, to make informed decisions.

So fundamentally, it's about data, being able to collect the right amount of data, filter and analyse it, and present it in ways that can be easily consumed, in text, graphs, infographics, etc. So, risk management is the whole workflow that allows that to occur. Basically, it's the workflow that allows the risk decisions to be made to match the risk mitigation for the company. And that's something that needs to be done from the lowest level of the organization all the way to the top. From individuals on the ground all the way to the board, the C-level executives and the boards. Who are the ultimate risk arbitrator for this whole operation.

So, traditionally, risk has been a very negative thing, because teams are allergic to it, nobody wants to own risk, and nobody wants to really embrace it head on, and usually, it becomes a big bureaucratic exercise, which is the worst part, a lot of times, it is not driven by reality, but driven, sometimes, by a perception of the reality. People can't get information, because the risk teams tend to be separate. It means they tend to live on a separate reality, because they don't get real data.

So real data, should be in real time, driven by the actual operational parts of where that data is created, that then feeds a whole number of analytics dashboards, that enables them to make good decisions. What we need to do from a group security point of view, is make this process clear and easy to use. We need to create an environment, that enables it to be effectively implemented in teams, they can move faster, because they know the rules of the game. They know how to get things done. They know the processes to go through and they allow, the systems to work without group security intervention. That's what you want. You want a workflow, where somebody wants to do something, the rules of engagement are not hard to find, they create a risk ticket, these are documented and go to the right person for risk acceptance in group security for approval. When tech ops for example implements it, using a very smooth process. In our case it’s going to be powered by a bunch of scripts that operate very efficiently.  And the compliance part is basically, the ability to map the current rules and regulations that we review, from a government point of view. The big core is the General Data Protection Regulation (GDPR), for example we are also Provider Compliance Assessment (PCA) compliant.

And fundamentally, I view compliance with GDPR as a competitive advantage, if we get it right, we'll be better than our competitors. We will be able to show that we care about data and our customers magic moments and be able to streamline a lot of the process. Because in a way, a lot of times, the reason why compliance is hard, is because we are looking for inefficiencies within the system. We are basically looking at parts of the business that maybe didn't have a certain level of maturity, or care, or focus. Sometimes, it's not the team that doesn't want to do something, it’s just they were not asked to do something, or it was not part of the business requirement.

What I like about the GDPR? It puts customer data, and the care of customer data, at the heart of what companies need to do. And this could either be a massive compliance problem and slowdown the business or it could be an accelerator. Going back to the car analogy, there a lot of security features in cars, like brakes for example, and others, that allow the car to go faster. That's what we want. We want the GDPR to be one of those features that allows the business to go faster. That allows us to integrate better with third parties, allows us to be much more efficient in how we create new projects. Allow us to share data more effectively and more efficiently, internally and externally. And to do that in a more secure way. So, there is a lot of great things that will come out of it.

And finally, it will allow us to plan for failure, in a much more efficient way, because we know there'll be issues, the question is how we handle and how we process those issues. So, for me, the Head of Risk and Compliance is somebody that will thrive on this challenge, and with technical knowledge, because a lot of these things are very technical. You need to be able to go down to the engineer level and be able to communicate with them and drive your point across.

And the reason why in my head, a perfect candidate has programming experience and knows how to program. This could be Python, or Excel or other languages, of course, JavaScript and Scala, would be more interesting. But, when somebody knows a little about how to program, it means they are free from the data. They look at a bit of data and go I can automate this, I can program that, and I can visualize this, and I can visualize that. And that's why programming makes the difference. It also a mindset that a programmer tends to have, with the ability to take a very complex problem and break it into small little problems, and solve them in sequence, and put them together again, which is how we program.

So, it’s the profile of my ideal candidate. And the interesting challenge now, is how do we create challenges that allow these properties and this thinking to come out. So, we can create a fair recruitment process that allows the perfect candidate to shine and to be obvious why that individual is the right one.

One more thing on the Head of Risk and Compliance, to be added somewhere in the middle before. The other thing this pro really needs a very high focus on details and process, and in law. Basically, this needs to be a Geek at reading law documents. Somebody that by their definition a good book is about GDPR. Finds it funny and enjoys the particularities of the law, and the idea of attending and participating in meetings about GDPR and writing articles, is something they will enthusiastically be looking forward to. And would love to be an active participant in the changing and interacting with the law. Basically, a Geek for law. and rules, in the same way that some of our members are geeks for technology and security.