ISO 27001 Case Study for Data Centers

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

CASE STUDY

May 19, 2014

INTERVIEW WITH GORAN DJORESKI:
ISO 27001 Case study for data centers

Interview by Dejan Košutić, September 5, 2013

Goran Djoreski is the CEO of the independent Data Center Altus Information Technology. Previously, he worked for 12 years in the financial industry, employed with Card business development, as well as the security of credit card payments.

In this interview we discussed which obstacles they found while implementing ISO 27001, and how they are using this standard to compete in the market.

DK: More than a year and a half has passed since you were certified by ISO 27001 – what are your impressions? Was it really worth it?

GD: It was definitely worth it, since it turned out that an ISO 27001 certification is not necessarily a competitive advantage, but rather a must-have. The background of the whole story is that we are trying to address the regulatory demanding markets. So we are talking about the pharmaceutical industry, telecommunications, financial industry, perhaps in the future also food production and similar, and they are all together extremely regulated, and in a conversation with them you find out that ISO 27001 is something they expect, or else they are not willing to talk to you. So one would not say it is worth it in the sense that it has brought customers to us; rather, it actually provided entry into a market we otherwise would not have had access to.

DK: Why are so many potential customers emphasizing ISO 27001; why is this standard accepted as something that is necessary?

GD: For them, ISO 27001 is often not enough. It is necessary, but not sufficient. They establish with ISO 27001 some initial level though, something like: "Now we can start to talk." If a company has an ISO 27001 certificate, they assume that some basic criteria are met, and after that, they're actually looking for their specific annex. In addition, the ISO 27001 process shortens their audit – which will now only takes two days, rather than six.

DK: Therefore, ISO 27001 actually is considered to be a baseline.

GD: That's right, a *baseline*.

DK: Is there some other standard appearing, which would be a baseline for these potential buyers?

GD: No, I would say that ISO 27001 is the main requirement. In particular, financial institutions usually look at PCI DSS, but since we are an infrastructure data center, we do not go into their data and transactions when delivering infrastructure, and if PCI DSS would be looked at, everything unrelated to infrastructure is out of scope for us. So they expect that with the ISO 27001 certificate, we have covered those chapters in the PCI DSS that are relevant for the infrastructure. They did not ask for ISO 9001 because they generally assume that if we have ISO 27001 certification, ISO 9001, which is important to them, is already included.

DK: If I have well understood your business, then you rent mainly infrastructure, so you don't handle data itself?

GD: In most cases it is so, yes.

DK: How beneficial is the ISO 27001 certificate for you as a provider of infrastructure services, if considered that this standard has a focus on information?

GD: I would say that ISO 27001 isn't based only on information, but also on everything that helps to ensure the safety and transfer of this information, and everything needed to make this information available, authentic, etc. In fact, the information as such is nothing; it cannot exist outside an infrastructure.

DK: In recent times, the trend has been more and more toward the cloud; how useful is ISO 27001 regarding this, or is it more of an obstacle? It could be an obstacle in fact, since the companies using cloud services actually lose control over their data.

GD: Actually not. If we think about the cloud in the way it is utilized by some of the big providers – be it Amazon AWS or Rackspace or similar – they highly industrialized their cloud, and they have a standard set of products, which address more or less the same pattern; this whole story is designed in a way to have data centers around the world, and they migrate virtual servers between them, so in fact, from this perspective it really looks like the users don't have control over their data. You can't know where they are, since today they are maybe in Johannesburg and tomorrow perhaps in Munich, and you don't have influence over the structure of the network, etc. That is a cloud.

But the cloud is also something else. Cloud is also what we do, but comparing to other suppliers we would make a distinction, like between tailor-made clothes, and industrially manufactured suits. So we cut and sew tailor-made networks: the user, who comes to us, agrees with us together on the structure of the network, where the virtual server are placed, and on the way, how the security will be dealt with. Of course, it all has to be within certain standards in relation to those big global players, since these are their servers and cities, etc., where the user's virtual machines are physically placed. We can define a framework, within which boundaries his cloud will be acting.

DK: Thus, in contrast to these large industrialized players there are also smaller players, who actually adjust the cloud to their specific security needs.

GD: Yes. Actually, in my opinion, in this kind of setup we have managed to reconcile safety and economy. The cloud significantly saves resources and thus makes it possible to reach the same level or a higher level of redundancy, and in case of failures and technical problems, the virtual server will continue to work on a completely different infrastructure and you don't need to buy 3 or 4 servers for this purpose. This means we align the approach with the fact that the environment, where everything is set up, will be controlled, so that you are aware of the fact that you might share a physical server with another user. But, on the other hand,

you know you have a completely separate network segment – that between you and anyone else there is a firewall, that it is in a cluster, where access is controlled, so that there is no possibility for someone to remove a drive from the server and put it back in place without control, etc. It actually gives the users a feeling that they have the same security like before, but with the benefits of using a cloud.

DK: OK, now I would like to talk about your experiences with the documentation. What surprised you the most? What did you get that was unexpected, and what did you expect and did not get?

GD: The biggest surprise during the implementation was that we thought we would simply get some kind of cookbook, and that there would be some kind of form, where we start from implementing a standard and go from point to point through it, following some kind of process, and we're done. But it turned out that this was not the case, and we had to start with a view of ourselves, so that was a big surprise for us. We did not get the definition of "ISO is that and that"; instead, we received "Find out first, what you need" and "What would you want from ISO in conjunction with that?" and we had to define ourselves how to implement it within the framework provided by the standard.

DK: Therefore, you had to start with risk assessment?

GD: Yes, risk assessment and before that with an analysis of our own business processes to even find out what the risks are. However, I did not expect that ISO would help us to facilitate operations, because one always sees ISO and all the other certificates as an additional burden; on the other hand, some unsolved things that we had fumbled and struggled with, we could regulate through defined processes, and now we know how it works in everyday business.

DK: How difficult was it to instruct your people to write documents, procedures and policies?

GD: It was not easy, and it actually is never finished. It's an ongoing battle. Initially, one needs to set up the rules for this segment, because if not, there will otherwise be no documentation. So it is a perpetual process, because you're fighting for everything to be as it should.

DK: Okay, but the question is whether the documentation is necessary, whether it is useful at all.

GD: This is another part of the story. No matter how much effort you invested, and the preparations can take 6 months or more, the documents may not perfectly match to what you are doing. Since your target is to get the certification, there might be a tendency to accept the things that are already written in the documents, although they are perhaps not perfectly tailored to your daily operations. Then it happens that a lot of this goes to the first certification round and the certification auditor asks: "Do you perform those things written in there?" And then you realize that nobody normal would do what is written in there.

And then in the next supervisory visit such things are lessened, because you are adjusting the documents to your needs more and more, because you have gained experience. But again there is a human need to get as much work done in a given time period, and the documentation is always an overhead.

DK: How can you solve, on a psychological level, this issue – that even if such documents are necessary, they are hated by the people who need them, who are pretty busy by the nature of the job?

GD: One should never be a slave to formality. I've already had experience with a company where a formal approval process was regulated in such a way that something had to be printed on paper in multiple copies, than be sent to 12 directors, who needed to read it and all of the 12 directors would have to sign it, and only after that it went to a committee – it was hell. It is normal for this to be a horror to the people. On the other hand, ISO 27001 allows, to a large degree, for a company to prescribe itself what is good enough, and in this

case you need to simplify the whole matter. You should not make an excuse out of needing 12 people to read and approve something, because of those 12, 9 members do not care about it. You should make the procedures easier and more effective, and begin to use the tools. Why would someone sign something on paper, if the approval through CMS is quite a sufficient tool? It means we have traceability, and we know that this is the man who signed and approved it, and we don't need to bring it to a notary public to prove the approval. And then people stop perceiving it like an annoyance, and begin to experience it as part of the process, and then everything gets easier.

DK: What was the most difficult thing during implementation? Was there anything that made you think of giving up?

GD: We did not want to give up at all, since we realized very quickly that it was to our advantage. Our motivation was the fact that if we wanted to deal with that, we needed this standard. This was never a question. What was the most difficult part? I would say that the most difficult was to assess the scope of the system, what we would deal with and how detailed it would be. There is a possibility that we will get an ISO documentation that is rated for a much bigger company than we are, and a lot of things were much simpler in our company, so we would need to cut a lot, but on the other hand, if you cut too much, and you check if you are conforming with the rules of the standard, it can happen that you have taken something out that was important. Here, your help was very welcome since you were goal oriented and said: "Don't think of that, it is not important for you," or "Those three documents you can merge within the operative structures," so that this part was pretty good. I think that during the implementation, especially when companies are working alone, there is a big chance either to be too extensive or to go below the required level. The borderline is not very clear and this made it difficult.

DK: How important is external help? Where's an optimum between two extremes – on one side, if you implement this standard alone, without any template and consultant, and the other extreme is, that you have a consultant who does everything for you. What is the middle ground?

GD: The first thing a company must do is understand this basic truth: a consultant will not do your ISO certificate. You will do your ISO certificate alone or not at all. Consultants don't do ISO certificates; you do your ISO alone, and the consultant recognizes your business processes. To be able to understand your business processes, it is necessary to employ a huge amount of consultants, and this is another job on its own. So this means, you do your ISO certificate on your own, with no consultants. A consultant is important in another area, and this is that the consultant understands the standard much better then you, and he can emphasize things you forgot or you perhaps exaggerated. The other thing is that a consultant gathered experience from practical work – in another analogy from traffic: theoretically, I know how I will cross the rail crossing, but if I don't know that in Croatia the ramp on the rail crossing often does not descend when a train is passing by, something very bad could happen. That is the same with consultants: they know from practical work what happened to others, where they ran into problems, either during certification, or in practice, where they oversized some things, and then such a security gap occurred, where they had damages measured in the millions. During the implementation we went several times in the wrong direction. We worked and heard suddenly – What have you done? Then we went two steps back and headed in the right direction again. If you don't have a consultant checking what you are doing on a regular basis, and who lets you go back two steps when you head in the wrong direction, it might happen that you have to go even ten steps back, and start again.

DK: Just to make it clear – is it the duty of the consultant to write your documentation or not?

GD: No. The document templates were of big help for us. Not so much because of the content, but to be able to see how this form needed to look and what topics needed to be contained with respect to the standard. Let's take the example of password policy; it is absolutely certain that the template where a password policy was described has nothing to do with what we do. So we made up a whole new story within the risk

assessment, and later in the description of our regulations of passwords, and at that place in the document we defined how we work with passwords – the text is probably 70% different from the one in the template. The very fact that we knew we had to write how we deal with passwords and that it needed to be in a specific part of the documentation helped us.

DK: That means, the templates give structure on one hand, and the freedom to describe what really exists in your company on the other hand?

GD: That's right.

DK: What is the role of the consultant in that case? If the consultant does not write your documentation, does he need to be present onsite in your company?

GD: No, he does not. We always wanted to have the consultant present, but he was not always here. We had a lot of meetings online. We loved to meet the consultant also in real life, but this has nothing to do with the very professional work, and more with the cultural background in Croatia – we love to meet a person in real life and to drink a coffee together. Actually, it was not essential to have him onsite because we were able to read the documents over a web screen, too. I would say, it is not necessary – pleasant, but not necessary.

DK: Why is the ISO 27001 certificate still not as popular as the ISO 9001 certificate?

GD: Probably due to unrecognized needs. The ISO 9001 certificate is somewhat like a shoe that fits every foot. Every company will recognize itself in the ISO 9001, but on the other hand, ISO 9001 is very often mentioned in public media. It is used like a marketing tool, like something very important. A third thing is, I think, that ISO 9001 can be implemented much easier than ISO 27001. On the other hand, to recognize ISO 27001 is much more difficult, no matter that I think that every company has minimum information within their house – we all have a minimum of accounting records, and a list of users with their phone numbers – and those are also data to be saved in security. Everybody could implement it. But there are only rare companies that need to implement ISO 27001 like we did, and when you take into account that ISO 27001 is much more difficult to implement than ISO 9001, it's logical that it is less popular.

DK: And finally, what are the 3 things you would recommend to IT companies that only started with the ISO 27001 certificate? What do they need to pay attention to before they start with the implementation?

GD: First they need to answer the question of why they want an ISO 27001 certificate, which means, do they want it, do they need it, and if they need it, how motivated are they to have it? This is to be done in the very beginning, giving pluses and minuses. Another thing is, if they decide they want to have it, then they need an absolute commitment of the Management to ISO 27001. There must not be any dilemma at any time, since during the discussion there will often be a moment to decide how to allocate the resources between projects, either to ISO 27001 or to another project that seems to be more important on first sight. The benefit of ISO 27001 is not that you will earn money when the project ends. You do it even though you do not see immediate benefits. This project can quickly get lost in a hidden channel. If you decide that you want ISO then the management commitment must be strong, must be stronger than others that directly generate income. The third important thing, in my opinion, is to pay attention to loose ends. Like with any project, with ISO 27001 you come up with some 95% of everything, and then have enough of the project and the certifiers and the internal auditor who asks stupid questions and then you still have to do 20 things, and you thought you had finished it. So you need to get through this finish line too, these last 5%, and then everything gets easier.

Sample documentation

Here you can **download a free preview of the ISO 27001 & ISO 22301 Premium Documentation Toolkit** – in this free preview you will be able to see all the mandatory documents required by ISO 27001.

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

EPPS Services Ltd.
for electronic business and business consulting
UI. Vladimira Nazora 59, 10000 Zagreb
Croatia, European Union

Email: support@iso27001standard.com
Phone: +385 1 48 34 120
Phone (for U.S. customers): +1 (646) 797 2744
Fax: +385 1 556 0711