Tessares share their ISO 27001 certification experience

Thank you to Denis Périquet, CEO (left) and Hugues Van Peteghem, COO, for sharing their experience!

Tessares is an SMB founded in 2015, focused on providing software solutions to telecom operators and ISPs (Internet Service Providers) to improve the Internet connectivity of their customers.

When we say 'improve connectivity,' for the moment we essentially mean boosting speed because not everyone is served in the same way. So, we combine several networks to improve the speed of the connection.

But improving speed can also mean improving the reliability of connectivity by combining several networks, because when you are connected to several at the same time, the probability of being disconnected is lower, as another network can always take over.

We also work on solutions that make it possible to switch easily and without interruption from one network to another, whether it be Wi-Fi, 4G or 5G, without the person realising that they are switching from one to the other while their smartphone applications are running.

We are based in Belgium with a team of around 24 people, among which some people are working for us from abroad, from England, Croatia and the United States. Our clients, as stated above, are mainly telecom operators in Europe in countries such as in Belgium, Finland, Lithuania, the Netherlands, Croatia and more recently we have also launched in the UK.

What were the reasons for getting certified?

It's not something that we necessarily sought to do initially, but it was pushed by one of our telecom customers, British Telecom. In the specifications they submit to all their suppliers, they require that suppliers demonstrate that they are meeting a series of requirements. So, in our case, being ISO 27001 certified was a specific request from one of our customers.

> *" It also demonstrates a good level of maturity in the company and increased our credibility on the market."*
>
> Hugues Van Peteghem, COO Tessares

What was the scope of the project?

Tessares is not a big structure, so we covered the whole company including our office building.

What was the necessary investment in terms of resources and time to complete the project?

From the start of phase 1 in September 2020 through to the end of phase 2 in March 2022, we spent more or less 1,700 hours working on the project. These hours were mainly worked by three people.

During phase 1, Approach was mainly responsible for the workload as this is the gap analysis to determine what the current security posture is and where we need to get. By February 2021, we launched phase 2 with the aim of obtaining our certification by the end of the year and so, from February to December 2021, that's when the vast majority of the hours were spent in-house.

There was a short gap between the two phases during the Christmas break and long enough for Approach to submit the commercial proposal based on the gap analysis since this report makes it possible to quantify the work to be done. And then, on our side, we had to make the decision and investment to pursue the certification.

Why use an external partner to support your certification process?

Thinking about it, it's really this idea of knowing where to start whilst not being aware of your incompetence on the subject. We knew that it was a subject that is quite different from our core business and relatively complex. Yet, it seemed to be a certification to get, so, we really wanted to be accompanied because we knew that we were going to go through all this questioning, and if we were not accompanied, we could have very quickly become discouraged.

So, we wanted to have the support of an external company. We also wanted a company that was not too big and that was aware of the specificities of an SMB and could accompany us and be agile with us.

Simply put, we were looking for a company capable of making us understand the complexity of what we had to do.

It's a bit of a shock, when you see the amount of work that has to be done. It was important to have someone to set up and then accompany us in these various stages. And then gradually bring us towards the competency levels needed so that we can manage this internally.

Defining a clear specification of what needs to be done for ISO 27001 is clear but the path to get to it is very unclear and that's where we needed guidance.

Based on what criteria did you select Approach?

> *" We looked for companies that could support us and that would pay attention to our company's profile, and in fact there are not many companies like Approach that will support SMBs in preparing for an ISO 27001 certification."*
>
> Denis Périquet, CEO Tessares

And then there is a certain proximity too. We are almost neighbours; we have common acquaintances who have worked with you in the past and shared a positive opinion on the service.

In your opinion, how did the project go?

We received useful guidance throughout; we really knew where to go and we knew very well what we had to do. The project was difficult because there was a lot of work to do. But that has nothing to do with the quality of Approach's guidance. We were warned that in phase 2, there is a lot of work to be done, a lot of documents to be read and created. Even if Approach provides templates, there are still plenty of things to put in place internally, and these are not easy things either.

We often faced resistance because security doesn't mean much to people. It puts obstacles in their way, and they can't always see any immediate value or benefit.

But we achieved the objective we had set ourselves. We wanted to pass the audit before the end of 2021. Following the audit which took place mid-December, we didn't get the certificate immediately because it takes time and there were a few points that we had to address. But we knew at the end of the audit that we had succeeded. We were incredibly happy to have achieved our objective.

What recommendations would you give to companies wanting to get certified?

You can't underestimate the project; you have to have a CISO who is going to take the project in hand. I think that in the run phase, you can think of an external person because everything is established and you just have to keep the boat afloat, but to first build the boat, it's imperative you have someone in-house.

You must set yourself objectives because if the project tends to drag on, the motivation will no longer be there, and it will become much more complicated to continue.

You must entrust the project to the right people in the company. Because if it’s entrusted to someone who is less involved in the company’s decisions, it’s likely not going to work because there are things to change and that makes people cringe, because we are going to disrupt everyone’s working habits in some way. So, if it’s not people with authority or leadership who come along and say, here we go, we’re going to do it, it’s likely to grind to a halt.

Here, we had two people from the management team involved in the project. So that’s really a recommendation to have the right people onboard and not just the CISO doing it alone.

And the second recommendation is to be accompanied throughout the process. I think that even if ISO 27001 is extremely well described, it’s still complicated. And discovering this path alone, I think it’s possible, but it’s just likely to take much longer, and with a higher risk of things not going well. In the end, the support enabled us to go towards this certification with only four minor non-conformities, which is particularly good.

Afterwards, we were also contractually committed to obtaining it. So, we had a real motivation too. But of course, I can understand that companies that don’t have this kind of obligation might want to deviate along the way and then drop out. It’s also perhaps a recommendation to know why you’re doing it. If you just say to yourself, this is a nice badge that I want to put on my website, it’s probably not enough. You need to have a clear purpose behind it and an understanding of what it does.

We were initially told we had to put the right people in place and the project was going to take time, it was going to be complex. But I think that until you’re at the bottom of the hill that you’re going to have to climb, you don’t realise exactly what it means.

In fact, you think, “Yes, actually, especially for a company like us. We’re a company of IT specialists with basic skills in many areas, but we weren’t fully aware of what that meant and the processes it entailed”. No matter how well it is explained, as long as we are not confronted with this reality, it is impossible to grasp exactly what it means. That’s when that support becomes essential, i.e., when we risk entering this potential phase of discouragement.

How likely are you to recommend Approach to your network and why?

We have already recommended Approach to other companies. As we said, we were well supported, the project was completed on time and within the budget, we are very happy with the collaboration.

About Tessares:

Tessares was founded in 2015 as a spin-off from UCLouvain. Tessares develops solutions for ISPs, MNOs, and MVNOs to deliver improved Internet connectivity by combining existing access networks.

Tessares' portfolio supports three main use cases:

- Seamless, overlapping mobile / Wi-Fi handovers to improve customer experience when moving between networks.
- Fixed-Mobile Hybrid Access to combine xDSL with 4G/5G for increased reliability and speed boost.
- MultiWAN solutions for Industry 4.0 which combine corporate Wi-Fi with private 4G/5G networks for seamless transitions and increased reliability in campus environments.

Tessares is a member of the European Innovation Council Accelerator Programme and our production customers include: British Telecom, Proximus, KPN, Telia, DT, Go Malta.

www.tessares.net

About Approach:

Approach is a pure-play cyber security and privacy firm.

For more than 20 years, we have been building trust in the cyberspace and helping our clients deal with cyber-attacks, incidents, and breaches.

We offer 360-degree solutions to improve your cyber resilience: anticipate, prevent, protect, detect, respond, and recover.

We provide tailored and local services matching your needs: consulting and audit services, training and awareness, security technology implementation and development services, and outsourced Managed Security Services thanks to our own Security Operations Centre (SOC).

Approach is a scaleup company with a team of a hundred people spread across several sites in Belgium and Switzerland. Our company is ISO 27001 certified and ISO27701 verified. Approach has received the label: Cybersecurity Made in Europe ™.

www.approach.be