BSI Customer Impact

CIRRITY

John DiMaria
BSI Senior Product Manager

Dan Timko
President & Chief Technology Officer, Cirrity

BSI Senior Product Manager John DiMaria sat down with Dan Timko, President and Chief Technology Officer at Cirrity to discuss the significance of the Cirrity's ISO/IEC[1] 27001 and CSA STAR[2] certifications. Timko detailed just how the certifications have enabled the channel-only, cloud service provider's partners and customers to experience the fiscal and operational advantages of cloud computing. Cirrity's high-performance infrastructure enables its partners to transform their businesses by providing them with a suite of secure and compliant cloud solutions and industry-leading service level agreements (SLAs).

JD: *When did Cirrity initially become ISO/IEC 27001 and STAR CSA certified?*

DT: It's been just under a year, actually. We were initially certified in July 2014, but we did our annual renewal and the upgrade to ISO/IEC 27001:2013 in May 2015.

JD: *For background, please share a little bit about the types of services that Cirrity provides to its customers.*

DT: We are a channel-only, cloud service provider. We provide our services through resellers in the channel market, which they then sell to their own end users. We offer three core service lines – Infrastructure as a Service [IaaS], Disaster Recovery as a Service [DRaaS] and Desktop as a Service [DaaS]. These three are a very good combined offering as they cover the full range of solutions that customers seek. This is one of our key differentiators when we are compared to most other cloud service providers.

Another big focus of ours is regulated end users, such as customers in financial services and healthcare. Serving those markets has been the big driver behind our security and compliance focus since Cirrity's inception. Both verticals have been driving a lot of our activity and growth. Our ISO/IEC 27001 and CSA STAR certifications have enabled us to go after that business.

JD: *When it comes to concerns about security breaches in cloud environments, it seems that when things do happen, some organizations choose to throw more money and more technology at their security problems. Is more technology really the silver bullet, or have you found that other factors are more important?*

[1] International Organization for Standards/ International Electrotechnical Commission
[2] Cloud Security Alliance Security Trust & Alliance Registry

DT: In general, people and processes are more important than technology. I think there is a place for good technology and it is required to fulfill the promise of the processes that are delivered. However, optimum results are more about the people that are implementing, managing and using those technologies.

If people are not trained adequately and the processes they use are not in place or kept up-to-date, the people themselves are generally the weakest link. They haven't been focused on securing all the 'layers of the onion.' Some of those layers end up getting overlooked because people think it is easier to spend money on technology and say they have accomplished something.

JD: *What are some things that Cirrity does to ensure that your people and processes are in tune with the company's overall security strategy?*

DT: We train. We provide awareness training and regularly update our employee base on the risks that are involved in their work. People who work here are continuously reminded that they have the 'keys to the kingdom', and, in a lot of cases, they are responsible for protecting our customers' data and operations. If those facts are kept at the top of their minds and they really understand their responsibilities as well as what is being asked of them, they are more likely to make better decisions.

Just attaining the certification helps us. CSA STAR is very different from other certifications because it is written with the intent of operating in a multi-tenant cloud environment. Most of the other regulations and standards are really focused on internal, singular organization processes. So, the road to getting our certification actually led us to make a lot of improvements. It also put us into a continual improvement state-of-mind. We are always re-evaluating what we're doing, looking at what's out there in the market, and thinking about what we need to do and what we need to be worried about.

JD: *What kind of regulatory requirements do you have to be concerned about and responsible for with your customer base?*

DT: The two biggest regulatory requirements for us are PCI [Payment Card Industry] and HIPAA [Health Insurance Portability and Accountability Act]. We have a large number of financial services customers that must adhere to PCI, FINRA [Financial Industry Regulatory Authority] and SEC [U.S. Securities and Exchange Commission] regulations. We also have a large number of healthcare customers with HIPAA-protected health information on the platform. Because our customers have these requirements on top of the platform, we have to build the foundation for them, and the services to support them, into our platform. We get into some other regulations, but PCI and HIPAA are the biggest.

JD: *Does ISO/IEC 27001 allow you to use it as an integrated system to help you ensure that you are meeting these other requirements in terms of controls?*

DT: Yes, internally they all kind of mesh together. ISO/IEC 27001 is a management system. One of the things we learned going into the certification process is that it isn't just about how the system operates and why. This certification is more about how the entire system is being managed.

We can take a step back and look at the system that is managing our information security, not just the information security components themselves. It gives us a wider, more top-end view. This allows us to better manage it from an organizational perspective and herd all of these different management requirements together under one common schema.

JD: *How do ISO/IEC 27001 and the additional rigor brought on by CSA STAR certification, CCM [Cloud Controls Matrix] in particular, make Cirrity a better organization?*

DT: In terms of ISO/IEC 27001, it makes us think about the system as a whole and how everything works together, not just system components. It makes us ask good questions, too. What are we actually trying to solve for? What are the risks presented by all of the seemingly random controls on PCI? We essentially have a list of controls to follow, which, if we had not started following them from the front part of the equation, we wouldn't necessarily know what risks we are solving for.

When we go through ISO/IEC 27001, what we look at is everything from start to finish, including what we are trying to control and what threats we are trying to protect against. The additional rigor of CCM within the CSA STAR certification is that it is very focused on the cloud service business.

Some of the other industry-specific certifications have that flavor, too. For example, PCI has an addendum for shared hosting and some other things that are specific as add-ons to the original. However, PCI is still intended to be looked upon primarily from the perspective of the company that is responsible for the actual financial processing activities.

Looking at CSA, it is easy to see that there is no shortage of controls. There are about around 130 now in 3.0.1, but they are written with the understanding that a multi-tenant cloud provider is addressing them. They are not written for an internal organization with its own set of employees, and maybe outside customers, to take into consideration.

As a multi-tenant provider, we have added challenges and ways we have to operate. We have multiple customers running on the same platform that we have to keep segregated from each other while we uphold our responsibilities to each of them. There are very industry-specific parts within CCM that help us to address these requirements.

Finally, customers want to know that not only that our platform is secure, but that there is not leakage between Customer A and Customer B, that Customer A can't cause a problem between Customer B, and that our employees are not going to get things mixed up and give their information to the wrong customer. These are just some of the things that don't necessarily come into play when you look at a standard or requirement that has been written with a single entity, instead of a multi-tenant entity, in mind.

JD: *Are your partners and their customers experiencing any benefit or ROI from all the extra steps that you have taken?*

DT: Sometimes, those steps are what actually enable them to move onto a platform like ours and get some of the benefits that cloud services provide. There is a huge ROI to the cloud in general, but if a company can't move to a cloud service provider because its platform does not meet their requirements, or have the level of assurance they require, the company can't achieve that ROI.

Because we have ISO/IEC 27001 and CSA STAR certification, as well as PCI and HIPAA compliance, our customers are able to enjoy the ROI and general strategic benefits of moving to a cloud offering. Depending on the kind of business they are in, Cirrity essentially removes a barrier to entry for them.

Hopefully, as we start to see larger enterprises adopting CSA STAR, it will become a requirement. Due to its focus on cloud and the openness around the CSA STAR registry, there is a ROI around vendor assessment for many customers. For example, they can rely on a company like BSI to come in and certify us a vendor. That means they don't have to do an audit, or regular audits, and pay for them.

Because we have done the groundwork and gone through these processes in order to certify our platform and our offering in general, that is a load off their plates. We look at it as making ourselves available to serve more customers and reducing the cost, time and resources required of them, because we have taken care of everything one time.

JD: *Yet, there are some cloud service providers that say there are enough audits now and they don't see any reason to adopt CSA or additional requirements. What would you say to them?*

DC: We still go through plenty of audits, but to me it depends on what we want our image to be as a provider and the customers we want to serve.

Cirrity attained its CSA STAR certification as a very proactive step. We are interested in what the CSA is trying to accomplish as an organization, and I believe the group is going to be successful. Having been to so many of the CSA congresses over the years, I have seen more uptake in terms of who is there and the number of people and the quality of attendees. Adoption is coming.

For us, it was a matter of being on the front side of that and showing we had that readiness in advance, versus having to lose customers first to feel that pain and then do it. I almost see it as something that is inevitable in our industry. Whether it's done in conjunction with the CSA or not, there is a lot of talk about the regulation of cloud.

For us, it's about future-proofing our business. If a company really believes in, and is diligent to the duty it has to its customers and protecting their data, then I think CSA STAR is definitely worth a look. It's a solid certification. You can't look at any of the CCM controls and say that they are unreasonable or that they do not need to exist in a cloud environment. If you can't say that, then why aren't you adopting it?

JD: *So Cirrity believes the pay-off will be much higher for the early adopters of CSA STAR than companies that chose to wait and see what happens?*

DT: Think about it. From a customer perspective, would most customers rather go with a cloud provider that was proactive in adopting a more transparent certification designed for cloud service providers, or would they rather go with a provider that had to be dragged to it kicking and screaming. What does that say about the latter? Are they more likely to be box-checkers in terms of meeting the bare minimum of requirements just to get certified? On the other hand, what does it say about the maturity and buy-in from an organization that is more proactive.

The value of the approach that we have taken, which is to build a secure cloud from the beginning rather than adding on security, thinking about it after the fact, or doing it because compliance demands it, is just part of Cirrity's DNA. It is how we believe cloud should be delivered.

bsi.

Your business could benefit from ISO/IEC 27001 and CSA STAR Certification just like Cirrity. To find out more, visit www.bsiamerica.com

BSI Group America Inc.
12950 Worldgate Drive, Suite 800
Herndon, VA 20170
USA

Tel: 1 800 862 4977
Fax: 1 703 437 9001
Email: inquiry.msamericas@bsigroup.com
Web: www.bsiamerica.com

BSI Group Canada Inc.
6205B Airport Road, Suite 414
Mississauga, Ontario
L4V 1E3
Canada

Tel: 1 800 862 6752
Fax: 1 416 620 9911
Email: Inquiry.canada@bsigroup.com
Web: www.bsigroup.ca
www.bsigroup.ca/fr

The BSI certification mark may be used on your stationery, literature and vehicles when you have successfully achieved certification and conform with applicable guidelines.

The mark shall never be applied directly on the product or service.