Integrating Third-Party Assessments and Regulations with CSA STAR and TokenEX
Introduction

What is CSA STAR?

The Security, Trust, Assurance, and Risk (STAR) Registry is a publicly accessible registry that documents the security and privacy controls provided by popular cloud computing offerings. STAR encompasses the key principles of transparency, rigorous auditing, and harmonization of standards outlined in the Cloud Controls Matrix (CCM). Publishing to the registry allows organizations to show current and potential customers their security and compliance posture. It ultimately reduces complexity and helps alleviate the need to fill out multiple customer questionnaires.

Interviewee:

Chris Dixon; former Governance, Risk & Compliance Manager at TokenEx

At TokenEx, Chris Dixon managed compliance obligations, monitored the data privacy landscape, and oversaw their BCDR Incident Management Response. He is now a senior compliance specialist at HubSpot.

TokenEx is a leading data protection and tokenization platform, founded in 2010. They can tokenize any dataset and help with the data protection requirements of CCPA, GDPR, and most other privacy regulations.

The level of STAR achieved

TokenEx completed the CSA STAR Level 1: Security Self-Assessment. At this level, providers submit the Consensus Assessment Initiative Questionnaire (CAIQ) to document compliance with the CCM. TokenEx also completed the CSA STAR Level 1: GDPR Self-Assessment, marking their GDPR compliance. Both of their submissions are publicly available on the STAR Registry here.
Challenges

What are the main security challenges that you face on a day-to-day basis?

Our customers are trusting us with their sensitive data. We really have to go out there every day and earn our customers’ trust and keep their data secure. Along those lines, we receive quite a few audit and due diligence requests from prospects, probably a couple a week. Our customers want to make sure that if they’re going to provide us with their sensitive data, it’s being secured and protected.

What was TokenEx’s main driver for adopting CCM and STAR?

The CCM is mapped to a myriad of different control standards. We have customers that provide different types of data that are in scope for a number of different regulations. By aligning our control framework with the CCM, we can display and show that we’re meeting all these different requirements. The STAR Registry puts a little more trust around it by publicly showing all of our controls that we have in place. We can stand behind what we’re doing.
Results

How has CCM helped TokenEx?

In some cases, the CCM eliminates the need for a formal questionnaire. We provide our CCM, customers look it over, and it addresses all their questions. That saves us the time of going any further. In some cases it will just reduce the workload or streamline the request. We provide them with the CCM, they look at their questionnaire, check off a number of the items, and then they come back and we discuss any questions they have. Even for customers that are going to conduct an audit or questionnaire regardless of what we provide up front, the CCM enhances our responses and supports what we're providing. So really it just increases that level of trust.

How has CCM facilitated some of your business targets?

As a business that sells a product, we have sales goals and want to meet them. By having the CCM assist with some customer audits, it helps the sales cycle move along smoother.

We've also used the CCM to aid us in other initiatives. For example, we're pursuing ISO 27001. We worked with the CCM as our core set of requirements since it has a bunch of questions around managing mobile and BYOD devices. We know if we include all these things in our policy and a few other requirements, we're going to be meeting ISO 27001. As we grow our program, we use the CCM to help us implement new policies and go after new certifications.

Were there any time or cost savings?

I'm not sure that you can put a price on customer trust. So really I'd say priceless. But I think a lot of it comes into the time savings. We go through a couple customer audits a week, so by reducing some of these with the CCM, the time savings definitely adds up.
Key Takeaways

What are the major benefits you see from using the CCM?

I would group it into three different categories. One that I’ve touched on quite a bit is providing assurance to customers. Another one is around board internal practice. The CCM is aligned with all these different frameworks and is updated pretty regularly. To be able to leverage CSA’s expertise and research to see what the best practices are across the industry, that definitely helps with our continual improvement and helps us to align with what the industry is doing.

The last part is around Third-Party Management. Our customers trust us with their data, and even if we’re going to be using a sub-processor, we’re ultimately still responsible for that. So it’s very key in our third-party processes that we make sure that vendors are living up to our security standards. The CCM can help us get a feel for their security controls and make sure that they’re living up to what we set for ourselves.

Listen to the full interview on the CSA Security Update podcast.