Mission critical cloud

It is not surprising that there is a lot of discussion in the industry today around cloud computing. What once was a speck on the technological horizon is here in a big way. In fact, many experts argue that cloud adoption is so widespread that we have reached a tipping point and can no longer call it an "emerging" technology. If this is true why are so many technology and risk leaders hesitant to adopt, or worse yet actively opposing, this powerful technology. Is it fear of the unknown or resistance to change? Or perhaps they know something the early adopters don't?

My colleagues and I have written extensively on *Building Trust in the Cloud* and *Governing the Cloud*. Through our research and experience, we believe that cloud is no longer an option; it is a strategic imperative. Many boards are now asking management about their cloud and digital strategy to take advantage of these advances. We encourage our clients to embrace the cloud, and where possible, think "cloud first" or at least strongly consider cloud-based options in their *make-or-buy* decisions. The benefits are just too great to dismiss. Yet the majority of the questions we answer are around "How can I get comfortable that my Sarbanes-Oxley (SOX) applications are safe in the cloud?" Better yet, "Can I run my mission critical applications in the cloud?"

We have debated this issue at length and weighed this question from numerous angles. I have spoken to many industry leaders in manufacturing, logistics, healthcare, technology and financial services and arrived at the same conclusion. In my mind the answer is straight-forward: you can put any application, infrastructure, platform in the cloud you want, *but (and it's a big but)* you must understand the controls that should be in place to support the requirements of whatever is going in the cloud. Easier said than done, right? Many of our clients ask whether SOC reports (SOC 1, 2 or 3), ISO certifications or independent testing results/certifications are sufficient to mitigate the perceived cloud risks. But certifications and third-party assurances are just half of the equation when building trust. The other half of the secret formula is the company itself, the consumer of the cloud services.

But doesn't the onus fall 100% on the cloud service provider to safeguard their customer's data and protect their critical business processes? Well, like all things in life: that depends. Certain controls are, in fact, executed by the cloud service provider (CSP) and typically they are done very effectively. After all, they are in the business of IT; it's their core competency. However, certain controls must be performed by the cloud consumer. Processes like access provisioning, periodic access review, role management, off-line backup/redundancy and encryption (just to name a few) often require an additional level of effort by the cloud consumer. We have found that companies that are good at these processes in-house are usually good at these processes in the cloud. But the inverse is also true and those who are not good at performing these processes in-house typically poorly perform these controls in the cloud. It is vital to understand *who* is doing *what* to draw a clear linkage between the controls performed by each party, the risks that are being mitigated and the risks that remain. Without this understanding, moving mission critical functionality to the cloud is like buying a house site-unseen without reading your mortgage documents. All you can do is cross your fingers and hope for the best!

But that still doesn't answer the question about SOX applications. When can we move those out of our environment and on to a cloud-based platform? My question to you is: what are you waiting for? Assuming we are talking about a reputable cloud service provider with a secure, trusted and audit-ready (aka STAR) environment, and assuming you (as the consumer) have done the due diligence of mapping

your old control objectives and control procedures to the new ones, I see no reason to wait. In fact, what we have found is the control objectives generally stay the same but the control procedures change to fit the new platform.

So, that's it really. A simple answer to a complex question of when can I move to the cloud? Now! But it should be done by carefully analyzing the controls in the whole cloud ecosystem, not only at the CSP, but also within your four walls.

justin greis

hi, i'm justin

(nice to meet you)

I post weekly **professional insights** and **personal stories** from my life as a management consultant, a dad, and an eternal optimist.

Click here to learn more about my **professional**, **personal**, and **"perfessional"** background.

connect with me

- **Visit JustinGreis.com**
- **Learn more about Justin**
- **Subscribe to newsletter**
- **Contact Justin**