Alex Brown: Hello. This is Alex Brown. Welcome to our continuing service series on cloud strategies for higher education. With me today, we have members from our IT consulting and cyber security team, Sri Chalasani, Donna Freddolino, and Kyle Macyda. Building upon our previous podcast covering cloud strategy, service providers, and implementation, we now want to share with you tips on structuring your service level agreement with cloud providers, including what metrics you will need to track, and best practice for ongoing management with your provider. Just one of these tips might save you a lot of grief. This topic is really where the rubber meets the road. To break it down for us, Donna, if you kind of give us just an idea of the development of the terms, what do you need to know in terms of setting up the terms and conditions?

Donna Freddolino: Well this area, Alex, is one where in the desire to get an agreement in place, many institutions almost proceed too quickly. They need to pause, they need to think about what the agreement is that they're seeking with a service provider. They often, in their haste, just ask a provider to give them the copy of the standard agreement or the standard terms that they use for the services that the institution is acquiring.

I have to say, that would be like only looking at one side of the coin. What we want to encourage institutions to do is to become more broadly educated about what they need to have in a service level agreement. We're going to give you some suggestions for what to include in there. Maybe draw upon resources and expertise from outside the institution, in addition to, for example, counsel, who might review one shared service agreement a year, to try and get some insights of what's emerging from other institutions, from firms like Plante Moran for example. We do a lot of agreement discussion and agreement review, and that of other institutions. Again, I go back to the educom site as being a really good resource of sharing about agreements that other institutions have established with other cloud service providers.

Fundamentally, I think it comes down to, once you have your plan in place, what is it that you want to include in a service level agreement? Sri, you've had a lot of success in talking with clients about that. I know you have some things that you really want to make sure are present in an agreement.

Sri Chalasani: Sure. I think one of the benefits of being in a cloud environment is you have the ability to look at each service independently. What I mean by that is you can look at an application, a process, or a physical infrastructure type system, and you can treat it with different variants of what you want in that service level agreement. For example, when you look at applications, we should not treat all applications equal, we should treat them dependent upon how critical those applications are. For example, a payroll or a ERP system, which has a broader impact on our user base, should have a higher level of criticality, compared to maybe a simple storage type environment, where we're exchanging files, such as a Google Drive or a Dropbox type of environment.

Donna Freddolino: You're saying like the metrics or the expectations for those would actually be different?

Sri Chalasani: They should be different. For example, your ERP system, if you say that one hour downtime is not acceptable, then your service level agreement should specifically say if the system is down for more than one hour, what is the vendor going to do to maybe reroute your traffic to a different data center, to bring your systems back up and running again?

You almost have to look at it in an application by application basis, or the service that they're providing, and treat it from your viewpoint as to how critical is it for your organization to have it back up and running.

Kyle Macyda: You often want to align those SLAs with the ones you may have internally, right? Making sure they're consistent, so if you have expectations from your institution that systems are available a certain percentage of time, or need to be back online, you'd want to make sure that what you're negotiating with your provider aligns with that, so that you're in sync, and there's not a big gap between the two organizations or the two infrastructure.

Donna Freddolino: Most students don't really want to accept any reduction in the total number of hours of IT technical support. They want, in fact, a 24/7 environment, so this is one which I think is a great example of where we're trying to get improvement by working with a provider.

Kyle Macyda: Yeah, and Donna, to your previous point about general counsel, typically clients will provide us feedback that the general counsel, they can review perhaps the terms and conditions, but technical SLAs about performance availability of IT systems, that's not really their language, and there can be sometimes a gap there.

Alex Brown: Right. I think one other thing, too, to add to that, is the aspect of regulatory requirements. If we're talking sensitive information, what are those critical regulatory things we need to consider in the SLAs? If it's sensitive health information that the medical school has, or we do a partnership, that that's taken to account for those areas that we need to protect. Same thing with if it's the storage of credit cards, which would fall under the PCI requirements, that we've kind of identified what needs to happen from the vendor's side.

Kind of stepping back, a lot of this, the SLA itself, the agreements we established kind of really formulates, if you will, the arrangements under vendor management. We're talking the relationship under how we maintain our relationships with our vendor. I know Donna, in our client experience we see a lot of IT relationships under the vendor management umbrella being a key driver to getting what we need out of our vendors in that relationship establishment.

Donna Freddolino: I think the key point to think through is, as we go with cloud providers we are making a fundamental shift in the responsibility to effectively evaluate how those services are being provided. We used to do that internally with our own staff, and now we have to have the knowledge, the expertise, and an assigned person who is capable for an external provider. Typically, a provider will assign some form of liaison, or a project manager, or a product manager, and have metrics that they are evaluating and providing on a monthly or quarterly basis.

What's really important is we need to make sure as an institution that we've got someone who's capable of reading and understanding those metrics, and taking an appropriate action if they're not headed in the right direction. It's a shift. It's a really important fundamental shift.

Kyle Macyda: Yeah, it is a shift. It's a shift, because traditionally IT was more of an operational role, and now they're ... That role is evolving into one that includes aspects of governance, and strategy, and vendor management, and delivering business value back to institution. The traditional making sure the lights are blinking, that's something we're now using a provider for, and so it frees up their time and their resources to deliver back to the institution.

Donna Freddolino: Absolutely right. It makes me constantly come back to, you know, what are the best practice metrics that I should be thinking about, or including? I'll throw one out, and that's because an agreement that I saw recently where a provider wanted to retain the right to aggregate information from a variety of institutions to do analysis. It was a little bit embedded in the agreement. Now, the institution saw that, they didn't want to have their data used in that way. I think it really makes a good sharp line point about what's in your agreement, what is the vendor allowed to do. I'd say best practice within certainly student, and other personally identifiable information, even if it's used in the aggregate, it would be likely a preference not to do that.

Alex Brown: Yeah, absolutely. We've talked about a relationship, but even when the relationship doesn't work out and we have to look at the exit strategy ... I know Kyle we've talked, and we see clients a lot of times where it's not the right relationship, and so maybe you can kinda give a little bit of that.

Kyle Macyda: Yeah, absolutely. I mean, obviously you want to perform your diligence, and do your work up front, and negotiate your terms and your SLAs, but the reality is if things don't go well, or there are chronic issues, and the contract needs to be terminated, what are those termination costs? What's your exit strategy? What do you own? What don't you own? At the end of the day you potentially could be walking away from agreement with no hardware or software licensing of your own. If you're lucky you'll have your data, but if your data's encrypted there may be challenges around making sure you have the encryption keys and things to extract that data. What are the provisions and costs for moving from provider A to provider B, or bringing things back in house? There's a lot of considerations there in really making sure that you have that dialogue up front when you're talking about governance and security, when you're talking about what architecture and what model do you use? These are additional conversations. It's often better to do it up front prior to when you actually need to exit, and trying to then negotiate because you're locked into a contract.

Sri Chalasani: One other thing not directly related to the exit strategy is also the data breach protocols. Obviously we never want to see anybody's data breached, but if it does happen where does the accountability lie? What is the responsibility of the provider to you? How quickly should they notify you so you can turn around and notify your constituents? How quickly do they react to a breech? Also, just worthwhile trying to find out when was the last known data breech within their organization, and how did they mitigate it? Finally, from your perspective what kind of technology, especially if you're onboarding a cloud service provider, what kind of impact does it have on your cyber liability coverage?

Alex Brown: Absolutely. I think that all these things, it sounds like it comes back to establishing and knowing what needs to be in our agreement from what our pain points are? Do we need back up in one day, or one second? Knowing what our rights are, what we can ask, and what's the kind of relationship we have, who to contact. Also, maybe the shared responsibility we talked about earlier about, do we have the right technical resources in house to understand, and understand what material reports are provided to us.

With that, I'll wrap this up. This covers our third topic in this series. As we step into our next series topic, which is covering cyber security, in that session we'll highlight special security issues, considerations that you'll want to be aware of as you define your cloud strategy. We know that as you continue to listen on, you're probably listening to this podcast on the go, and may want more details or checklists when you get to your desk, so please feel free to go out to our website and we have information there available for you for reference.

With that, I'd like to thank our panelists here. We will look forward to seeing you on the next podcast. Thank you.

Announcer: Thank you again for joining us today. For more information on higher education please visit highered.plantemoran.com. Thank you.