The Cloud Is A Win-Win For Government, For Providers, For Americans

If you are a cloud provider take note: NO CIO is really going to strongly consider a technology that is not FedRAMP certified at this point.

Gone are the days of deciding whether or not to migrate to the cloud.

Now it's more about strategies on migrating to the cloud ASAP. So when migrating to the cloud, it's paramount to make sure your cloud assets are in a secure environment. And that was always the debate. Can I assure that if I put my crown jewels, my critical assets, into the cloud, they will be secure?

That mindset has changed; the thought process is not only is the cloud secure, it's actually more secure and less risky than keeping it in your legacy environment. Why? Simply because you can't afford to try to keep up with these bad actors. And there's not enough guards, gates, and locks, and technology that will protect your legacy environment. We know that these clouds are rock-solid, bulletproof in most cases.

Luke McCormack
CIO (retired)
Department of Homeland Security (DHS)

So, number one, migrating to the cloud is a solid decision to make. Number two, to have these products and goods in environments that are FedRAMP certified was always part of the dynamic.

The days where many of these products were pending FedRAMP certification are gone as well. Most of these capabilities, products and services you buy today are FedRAMP certified. And I tell this to the various partners out there. No CIO is really going to strongly consider a technology that is not FedRAMP certified at this point.

There is also a place for a hybrid environment — where there are a lot of assets still in these federal legacy on-premises environments and some assets are in the cloud. This works because there's a lot of technology now that is stitching those two environments together into this seamless type of atmosphere and experience. So you can't even really tell whether or not it's actually running on premises or it's running in the cloud, because this technology allows that to be ubiquitous. And that's an extremely powerful type of environment having that type of operating system.

Don't Learn The Hard Way

The other important thing that unfortunately some folks learn the hard way is: "Hey, you can't just take your critical assets, your most critical, high-valued assets as the federal government has categorized as, put them out into the cloud and say, 'Hey, I'm all done. We know the security's out there. We know that these various cloud service providers are going to take care of that. They're FedRAMP certified and we've relinquished our responsibilities.'"

There's no question you must provide good oversight as any smart buyer of these different goods and services would do. Ultimately you're responsible as the CIO, the CISO, etc. for that technology. The bottom line is: it's essential you maintain that level of oversight and ensure the integrity is in those environments.

Each Multi-Cloud Environment Must Be Learned

Learning to operate in a multi-cloud environment is critical today. Over time, most agencies have discovered they are operating in a multi-cloud environment. Agencies will use Office 365, which is running in the Azure environment. And then they may have some goods and services that they've bought — for example a Software-as-a Service (SaaS) — running in an AWS environment. So by default they find themselves in a multi-cloud environment and that's okay.

"There's no question you must provide good oversight as any smart buyer of these different goods and services would do. Ultimately you're responsible as the CIO, the CISO, etc. for that technology.

It's only when agencies get into situations where they are doing more of an organic build — for example, a bottoms-up build on a business application that they run in AWS. And so they're familiar with all the bells and whistles and knobs that they can turn; and how to manage that and how to spin environments up and shut them down. These are the intricacies of operating in an AWS environment.

But for a different application, they may go to Azure or Google and say, "Okay, we kind of understand that. We know how to do organic builds. We're now going to do one into Google environment. We have our cloud engineers, the site reliability engineers, etc. that know how to do this."

When they actually go to Google to build the application, it's like: "Hmm, that knob used to look like this and turn like this over at AWS. And that's different over here." This is obviously simplifying this. The point is agencies have discovered that is quite a bit of a learning curve to take that same level of expertise and fine-tune it for a second cloud or a third cloud.

Again, you can do it in more the default Office 365 or a SaaS service because you're extracted from all that. And you're just buying it as a full service. But when you get in there and you build these organic builds in those environments, you must learn the intricacies of those cloud environments. And they're not the same. And that is a discovery curve that all of these more advanced agencies are finding themselves in.

That's okay, because having multi-cloud environment has a lot of advantages. But there's some things that you have to be prepared for and skilled for — whether it's organic cloud engineering skills or tools, for both those environments.

I Call It Nirvana

What a lot of agencies would consider somewhat of a holy grail is: If they have a multi-cloud environment, they can take that a particular computing capability that was built to run in AWS and then magically slide it over to Google, or go half and half.

That is a difficult situation. Again, there's a lot of technology out there that makes that much better.

Some of it's that same sort of hybrid-type technology. But that is not an easy environment to master, but ultimately, one that a lot of agencies are seeking. I call it Nirvana. I'm not sure that's the right way to describe that because it's more of a necessity for checks and balances, so you don't have vendor lock in.

Then there is pricing. There was this idea that, "Okay, I'm spending an a huge amount of money trying to run my own environment. I'm not even sure it's secure as a cloud environment, or I've gotten to the point where I realize it probably isn't." It's sort of an arms race as far as funding is concerned.

> Cloud is going to allow the government more than the private sector to really accelerate their business systems at what we like to call the 'speed of mission'.

In some cases, they're allowing their developers to go out there and fire up these various servers in these cloud environments — until they see the bill. So a lot of agencies had to learn how to be a little bit more efficient, even though it was elegant and certainly a rapid way to develop. Some guardrails had to be built around that.

Thus technology was introduced to meter usage, because if things didn't get turned off billing continues. There were lot of early adoption lessons learned so that now you're getting the most out of these cloud environments without paying the penalties.

Win-Win For Citizens

Cloud, overall, has been an absolute win-win. We went from Cloud First OMB guidance to Cloud Smart. That means you're not going to just run yourself into the cloud. You're going to think that through, and you're going to decide if I want to use some hybrid, if I want to use one cloud or I want to use a multi-cloud. But whatever choice, I'm going to be smart about it when I think it through and be real purposeful about when I go into the cloud and what do I put in the cloud and which cloud service providers I use.

Cloud is going to be something that is going to allow the federal government, in particular, more so than in the private sector, I would say, to really accelerate their business systems at what we like to call the 'speed of mission'.

The time and energy it takes to procure all these goods and services to create the environment you need to build these business systems is enormous. And if you can take a lot of that away and just sort of buy that as a service, that's an incredible advantage to the federal government, which means an incredible advantage to every citizen out there that gets to enjoy those services sooner rather than later. ■

Luke McCormack is National Director of ACT-IAC. He also serves as the National Director for the U.S. Cyber Challenge. Mr. McCormack retired as the Chief Information Officer (CIO) at the Department of Homeland Security (DHS), where he provided strategic direction, cyber security services, oversight to cross-component information technology efforts and IT Cloud/infrastructure services. He also served as the Vice Chairman of the Federal CIO Council. Prior to this appointment, he served as the Department of Justice Deputy Assistant Attorney General for Information Resources Management/Chief Information.