

by **Evan Schuman**
Contributor

Signing up with a cloud provider? Don't forget to set an exit plan

Opinion

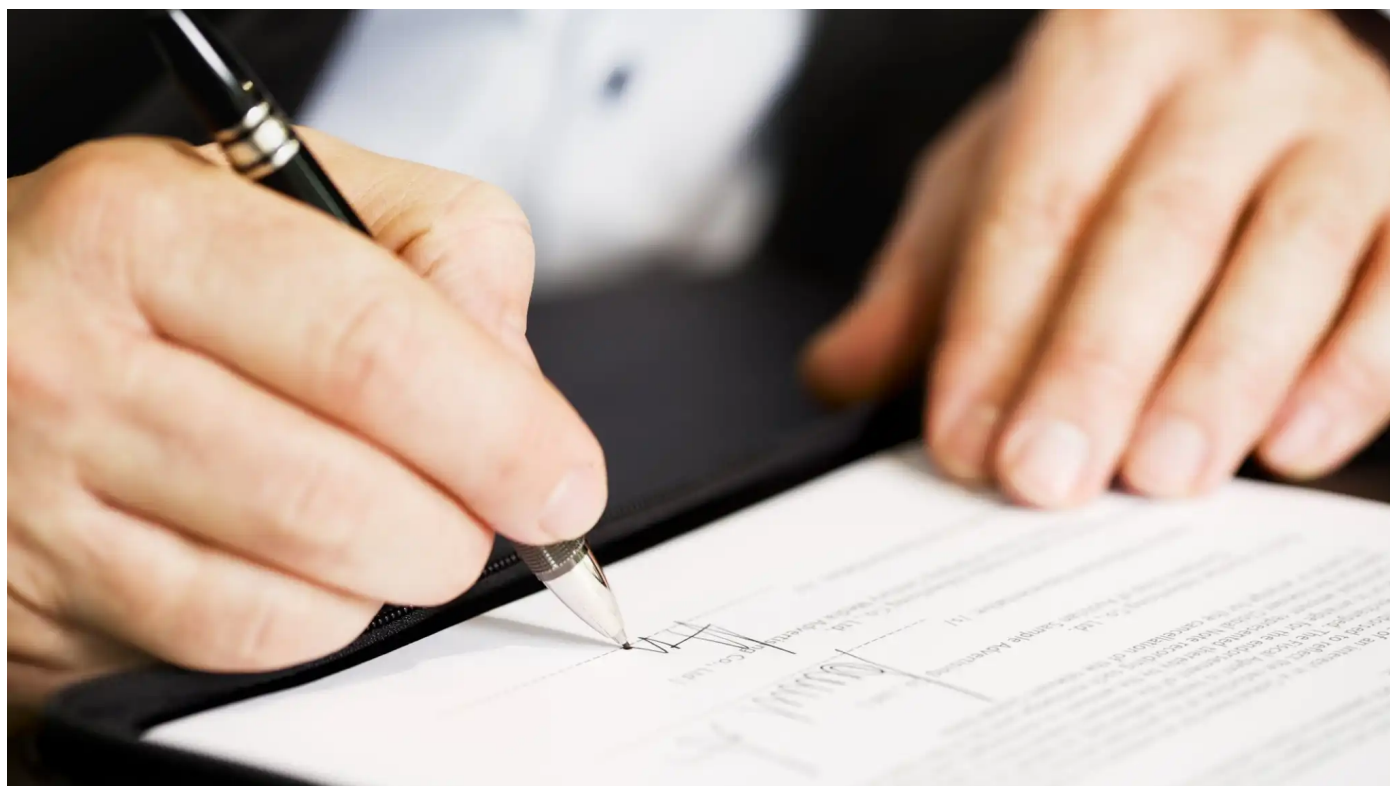
Feb 22, 2022 • 5 mins

Cloud Computing

IT Strategy

Technology Industry

It's not simply about getting easy permission to go when it's time to part ways; it's about IT making sure any decisions don't complicate that eventual departure.



Credit: Thinkstock

In my last post [<https://www.computerworld.com/article/1617582/rackspace-is-now-the-roach-motel-of-cloud-platforms.html>], I wrote about a cloud platform (Rackspace) that made leaving its environment impressively difficult. So it makes sense now to explore ways companies can better prepare for an exit — and precisely how to exit when the time comes.

The problem is that few legal departments focus enough on **exit details** [<https://www.infoworld.com/article/2269192/when-a-cloud-provider-retires-a-service-youre-using.html>], especially when they just negotiated a new, long-term agreement. It's not merely about getting easy permission to depart; it's also important that IT ensures that any decisions don't complicate things when it's time to make a break.

Complex global cloud arrangements can get complicated in 2022; the trick is that cloud-based capabilities that make data-sharing and data-protection efficient and friction-free tend to include lots of proprietary elements. Those are precisely the kind that tend to lock-in an enterprise and complicate a departure down the road.

Cloud providers “make it easier for you to use their native services,” which are invariably proprietary and have a degree of lock-in, said Rich Cracknell, a cloud security leader at McKinsey's Silicon Valley office.

Cracknell's McKinsey colleague, Justin Greis, added that these cloud services can be “highly dependent (on that cloud environment) and tightly coupled. You need to do an app-by-app analysis to see how tightly coupled each one is. Do we refactor it now or do we move it as is and kick that can down the road?”

The reality is that most enterprises, especially in the Fortune 500 and larger category, are going to already have a cloud presence with multiple cloud environments. That ideally means that IT already has an excellent sense of how the major platforms differ. That said, when it comes time to move from one to another (said Greis: “Amazon doesn't necessarily play well in the Google world”), unpleasant surprises are all but certain.

This brings us back to the key point: What terms/language do you want in cloud contracts to make the inevitable exit easier?

Many people who've dealt with cloud issues talk about the level of assistance the exiting cloud vendor should provide in the move to a new provider. That raises a suspicious issue: Do you really want the cloud vendor you just fired to be involved in the transition at all? In a perfect world, that help would be critical. But in the real world, doesn't the fired cloud vendor have a conflict of interest? Would they be happy if the new cloud environment never worked as well as theirs?

There are also compliance and security risk issues. During a transition, your most sensitive regulator-overseen data will be in two places at once, potentially for weeks and maybe months during the transition and testing stage. There is little to no alternative than to temporarily have double-data, but it is a risk and compliance issue that needs to be presented to those areas.

Todd Smith, senior vice president and general counsel at contract lifecycle management company Icertis, offered a suggestion that may soon no longer be relevant.

Computerworld Smart Answers [Learn more](#)

Explore related questions

- [How can enterprises avoid vendor lock-in when using cloud services?](#)
- [What are the consequences of not having a clear exit plan when using cloud services?](#)
- [What are the benefits of using a cloud broker to manage cloud services?](#)
- [How can enterprises negotiate better cloud contracts to reduce the risk of vendor lock-in?](#)
- [How can enterprises ensure a smooth transition when moving from one cloud provider to another?](#)

Ask a question



“It is much less common these days, but occasionally a customer will ask for a source code escrow. In theory, this would permit the customer to run the (environment) on their own if the vendor ever goes out of business,” Smith said. “That ask is far less common today because most understand SaaS isn’t instrumented that way and the subscription model makes the commitment lower on the front end anyway.”

There are many reasons to want to leave a cloud platform, but it’s important your contract specify the right to leave for convenience — meaning without any particular reason. It’s sort of the cloud vendor contract equivalent of at-will employment.

“Without this provision, you as the client company will be forced to show cause when you want to terminate the agreement with the service provider for not meeting your stipulated expectations. Showing cause is a very difficult and time consuming endeavor for the client company,” said Ben Richardson, senior software developer at security vendor SecureW2. “You also want to ensure that the agreement clearly stipulates events that are considered a fundamental breach of the contract by the service provider. These events may include data loss, inconsistent service provision, data leaks, data misuse, and violations of personal data protections. Go over the events listed and ensure that every event you consider to be a breach of contract has been included.”

Mark Rasch, the head of the cybersecurity practice at law firm Kohrman, Jackson and Krantz and the former head of the US Justice Department’s high-tech crimes unit, argues that the contract should also focus on rights and ownership issues regarding everything in that cloud environment.

“The fact that you own the data doesn’t mean that you have the ability or the right to move it from one place to another. Ownership is a copyright concept and control is a physical concept. Include a data portability clause,” Rasch said. “You want to make clear that my data is my data, as well as apps as well as specialized APIs to make my data useful. Who owns those APIs? You didn’t write them.”

Rasch also suggests that the contract also explicitly address how any and all items in the cloud environment will be handled. “Upon termination, everything will either wiped or encrypted. Talk about what happens to the data after you leave. Detail liability if it’s not wiped and it later gets breached. Make sure that the contract requires that everything also be removed from all backups and all of the archives.”

Sponsored Links

Secure AI by Design: Unleash the power of AI and keep applications, usage and data secure.

Empower your cybersecurity team with expert insights from Palo Alto Networks.
