10 BEST PRACTICES TO AVOID CLOUD VENDOR LOCK-IN

In the cloud world, our workloads exist wherever we operate: across hybrid clouds and various managed services. But if you've ever tried to move a workload or dataset from one cloud to another, you might have come up against some tricky terrain. This challenge—moving your workloads from one cloud vendor to another—is known as vendor lock-in.

Vendor lock-in occurs most particularly in cloud computing, where users are encouraged to sign up easily, but a variety of practices make it harder for users to "leave", move data. Fortunately, there are steps you can take to avoid cloud vendor lock-in. Let's take a look.

What's vendor lock-in?

Vendor lock-in refers to the restrictions that prevent users from switching a service.

In an ideal open IT environment, users are able to "lift and shift" freely as they want—they can migrate data and IT workloads from one technology stack to another, between competing vendors and geographic locations. The world of enterprise IT, however, is not always open. This is especially true when proprietary technologies, fierce market competition, and regulatory restrictions are involved.

Some vendors make it particularly difficult for their users to migrate IT workloads off to a competitor's service stack. Accepting a user's right to do so freely means lost revenue streams when users don't commit to long-term business partnerships. However, vendors never explicitly prevent users from practicing this freedom; they merely impose technical, financial, and legal restrictions

that discourage users from doing so.

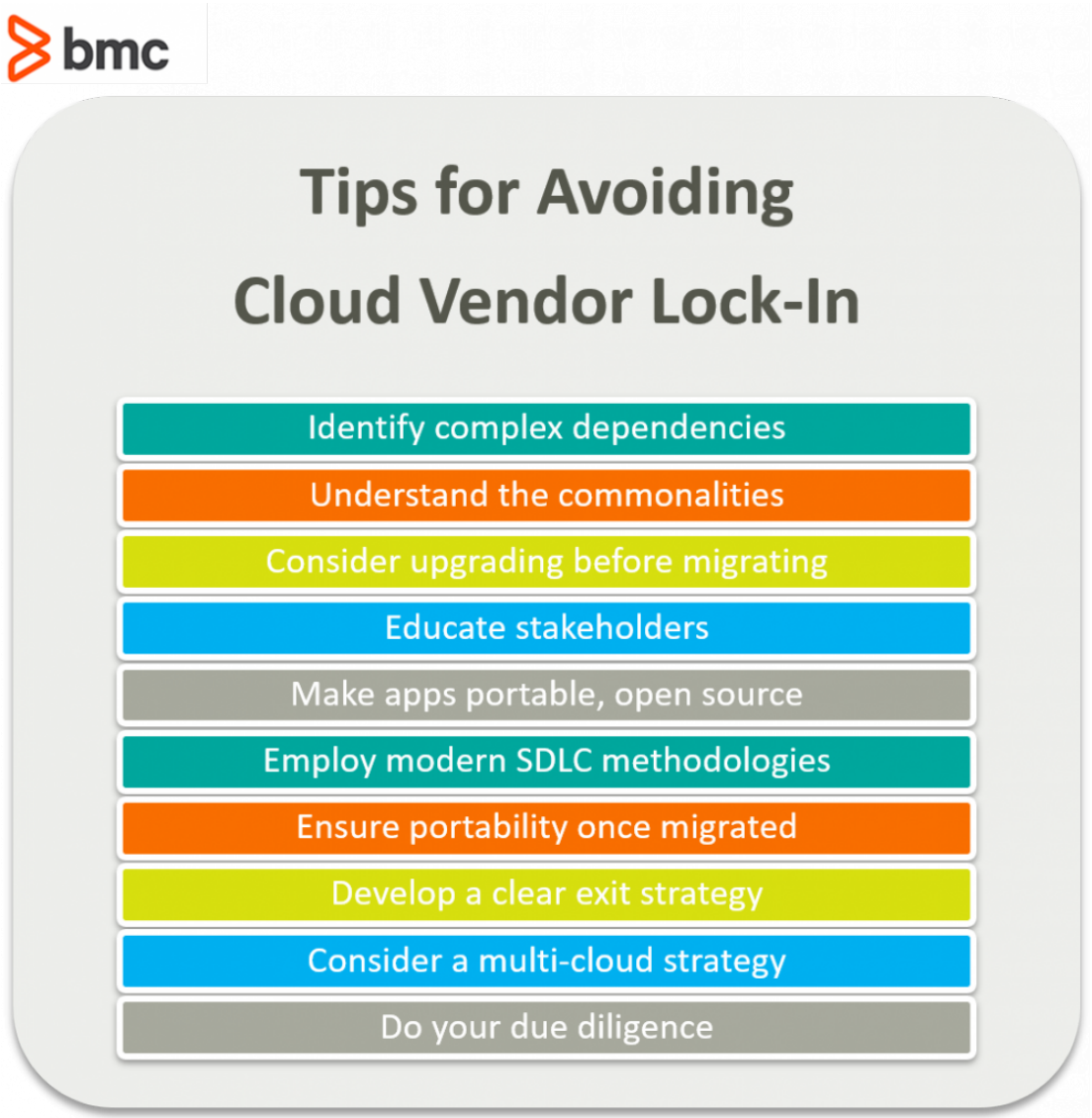
Conversely, vendors make it easy for users to join their service:

- Initial costs to start computing is kept low. But—it increases exponentially when users need to scale the service.
- Technical limitations such as performance, security, integration, and compatibility issues with technologies from competing vendors are only experienced at a later stage.

In many ways, these limitations are either specified as obscure fine print details in their Terms of Service (ToS) or cannot be foreseen as a user's technical requirements evolve unpredictably.

Tips for avoiding vendor lock-in

Vendor lock-in an oft-cited reason against cloud migration. In fact, the concept of lock-in altogether negates a primary value proposition of the cloud: its flexibility. However, there are ways to reduce the risk of vendor lock-in by adopting the following best practices.



1. Identify complex dependencies

Review your existing technology stack. If your IT workloads are designed to operate on legacy

technologies, your choice of cloud platforms and infrastructure will likely be limited.

2. Understand the commonalities

Compare what's compatible across cloud vendors, your existing technology stack, and your technical requirements. These commonalities are key to determining the best cloud solutions for your business needs. If there isn't an alternative service available, then you must rethink your IT strategy, your decision to migrate, and the technical requirements of your IT workloads.

3. Consider upgrading before migrating

If your apps are compatible with only a limited set of technologies, you may want to first consider upgrading or reworking significant proportions of your apps before migrating to the cloud migration. If your apps and IT workloads only work with legacy technologies that are supported by some cloud vendors, your future requirements to scale the service to an expanding user-base may incur a high financial cost or technical challenges.

4. Educate stakeholders

Training and stakeholder engagement are critical to understand the unique risks of vendor lock-in facing your use case. Tech teams should be aware of the business implications of their technical decision choices. A working solution in the form of apps, IT workloads, or computing architecture should align with business requirements and risk. Before migrating IT workloads to a cloud service, carefully evaluate vendor lock-in concerns specific to the vendor and the contractual obligations.

5. Make apps portable, aligned with open standards

This practice ensures a variety of cloud alternatives. Many cloud vendors support most open standards across various industry verticals. Switching vendors easily and effectively is easier with sufficient alternatives available. For this to happen, your IT workloads must support non-proprietary alternatives. If your workloads are locked-in with the APIs, configurations, and features of proprietary technologies that don't support open standards, vendor lock-in is likely. Failing to support open standards may require heavy customizations at a later stage to escape a vendor lock-in situation.

6. Employ modern SDLC methodologies

Designing according to modern SDLC methodologies gives you flexibility. For example, DevOps not only encourages the use of open-source technologies but focuses particularly on the technology-independence of cloud service management and operations. Consider Infrastructure as Code (IaC), a common DevOps practice for provisioning, managing, and operating infrastructure. IaC automates the process of describing infrastructure configurations and dependencies converging from an arbitrary set of choices to a repeatable desired state of technology-independent design.

7. Ensure portability once migrated

Transferring data from one service to another, as long as it stays with the same vendor, is often free. But, when migrating to a competing service, this transfer is charged steeply. Evaluate and consider these costs before migrating to the cloud, based on future requirements to scale cloud-based data

storage and related services.

8. Develop a clear exit strategy

Cloud vendors can go out of business or make drastic changes in their ToS within their legal rights—even at the expense of their users. You can reduce this risk by establishing a possible exit strategy. Feasible terms for contract exit should be agreed by both parties to make it easier for customers to avoid a situation of vendor lock-in.

9. Consider a multi-cloud strategy

Take advantage of multiple cloud services and distribute your workloads independent of the underlying vendor infrastructure. A multi-cloud strategy requires organizations to take additional steps in optimizing for cost, performance and risk such as vendor lock-in. By getting it right, several aforementioned risks are naturally addressed as your apps and data can operate on a hybrid mix of multiple cloud platforms by design.

10. Do your due diligence

The following items should be a part of your due diligence strategy:

- Establish a thorough and accurate understanding of your technology and business requirements. What is expected to change and how?
- Assess the cloud vendor market. Audit their service history, market reputation, as well as the experiences of their business customers.
- Understand trends in the cloud market, the business models, and the future of cloud services.
- Understand the legal limitations applicable to your cloud use cases. Are there unique regulations applicable to the vertical of your business domain and IT workloads?
- Read the fine print. Agree to Service Level Agreement (SLA) terms and contractual obligations that limit the possibility of a vendor lock-in scenario.

No magic bullet for avoiding lock-in

Finally, it is important to understand that taking extreme measures to avoid vendor lock-in can have unwelcome consequences. Going open source doesn't magically eliminate vendor lock-in. In some cases, proprietary technologies may offset the performance, cost, or security risks to specific open-source technologies.

Or, perhaps, present another lock-in situation different from proprietary vendors. For example, you can switch from proprietary AWS technologies to Kubernetes as an open-source solution. As your applications scale and increase in complexity, managing all those configuration dependencies and YAML files to switch from Kubernetes to another open source or proprietary alternative may be a huge challenge for your IT teams. In this case, it may only be a matter of replacing one lock-in with another one.

Additional resources

For more information on making the cloud work for your company, browse the BMC Cloud Blog or check out these articles:

- Public vs Private vs Hybrid Cloud Differences
- Public Cloud Growth Trends and the Future Outlook
- Hybrid Cloud vs. Multi-Cloud: What's the Difference?
- How Multi-Cloud Can Enable Cost Savings
- SaaS vs PaaS vs IaaS: What's The Difference and How To Choose