MassBio
MASSACHUSETTS BIOTECHNOLOGY COUNCIL

ECI

4 Common Cloud Migration Fears—And How to Overcome Them

Migrating to the cloud is often accompanied by an array of hopes and fears. The cloud promises flexibility, scalability, and increased efficiency. Investment firms can shrink their data center footprints and better support clients in today's digital-first world.

But change of any kind is scary—and uncertainty often breeds fear. Is the cloud less secure? Will we be able to stay compliant? Such questions circle cloud migrations like a hawk.

Cloud migration frameworks are meant to quell some fear about the process. Microsoft and AWS both offer frameworks that break cloud migration into four broad buckets: assess; migrate; optimize; and secure. While these frameworks are helpful, far more detail is required to ensure a successful migration in the Life Science space.

Let's look at three of the most common fears you may have around cloud migration, and how existing frameworks can be better applied to overcome them.

1. Costs

Most COOs and CFOs are used to a flat run rate for IT spend. Legacy IT infrastructure relies on a CapEx model, where they spend more upfront and enjoy economies of scale over time. But the cloud runs on an OpEx model. You spend less upfront and are billed based on consumption, which can fluctuate. Fluctuations can be particularly scary for Life Science firms, which must keep track of every penny. But the cloud offers a leaner IT balance sheet in the long run.

Modeling how this shift will impact budgeting and corporate accounting is an important step—one that should take place during the assessment phase. To properly calculate total cost of ownership, it's crucial to account for all pieces of the puzzle, including bandwidth, utilization, and storage.

Start by calculating the cost for the first three years of cloud usage, with projected growth on utilization and data. But also, understand that it usually takes three to five years to see ROI. Be prepared to give it time.

2. Disruption

Migrating to the cloud can be a disruptive process if not done correctly. Minimizing disruption requires sufficient strategy and assessment—the first bucket of cloud providers' frameworks.

Start by unwinding your existing infrastructure, so you know where things stand today. How are things running? How do people access data? How might your infrastructure change over time? Perform a full inventory and determine what data needs to be moved to the cloud to minimize disruption.

Additionally, be prepared for operating and support models to change. Consider ahead of time what training, integration, and alerts are needed to keep things running smoothly.

When it's time to migrate, develop a training plan for staff. Start small and staff the cloud migration as a project, embedding existing team members where possible or applicable so they gain invaluable cloud experience.

But migrating isn't the finish line. The next bucket is optimization, which should be an ongoing and continuous process. The cloud evolves quickly. Having a continuous process for optimization ensures you're running in an optimal state and are aware of new functionalities.

3. Compliance

You might also be concerned that migrating to the cloud may lead to non-compliance and firms cannot afford to have that happen as they focus on their operation mission. That's why, just like with cybersecurity, it's important to consider compliance from day one.

ECI recommends that all policies and procedures should be updated, especially for workflows that impact general ledger and financial statements. Further, governance documentation should include controls that have been established, including change controls, signoffs, and approvals. Proper history of change controls should be maintained for auditors down the line.

4. Security

The cloud is highly secure, yet there's a general perception that data stored in the cloud is more exposed than data stored on-premises. But consider this: when there was a big vulnerability in Microsoft Exchange, Microsoft patched the cloud vulnerability within hours. They didn't patch the on-prem vulnerability for three days.

Cloud migration frameworks save security for the final bucket. But in the Life Science world cybersecurity must be considered from the very beginning.

Your firm must take some responsibility here. Don't relegate all security to your cloud provider. Instead, implement cybersecurity platforms, proactively monitor for misconfigured devices, and ensure proper controls have been implemented so teams do not accidentally expose assets to the Internet.

The best thing you can do for security, though, is partner with someone, like ECI, who has experience with cloud migrations. This allows a secure framework to be deployed from the get-go, with code used by many clients already.

If you're fearful of migrating to the cloud, you're not alone. But between existing frameworks, savvy partners, and careful planning, most major risks can be mitigated. You can reap the many benefits of the cloud without being kept up at night with worry.

We can help. For more information on ECI's cloud migration services, contact us today.