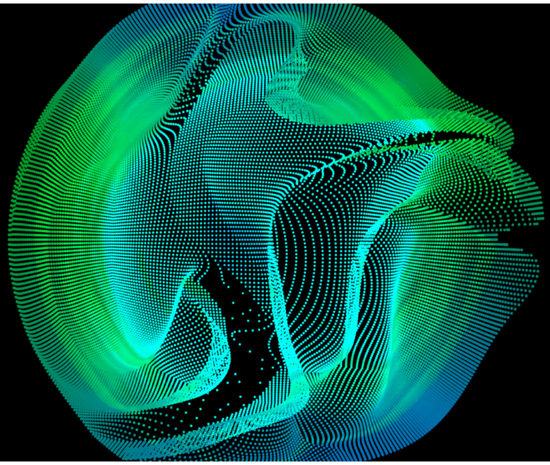
Deloitte.

Enhancing your enterprise IT: Four things you can do today to help bring about a successful post-COVID-19 recovery



David Linthicum, chief cloud strategy officer, Deloitte Consulting LLP

Over the past two decades, we've encountered economic downturns, natural disasters, and terrorist attacks. Now, we can add a global health crisis to that list. And while all these events bring hardship and heartache, there are nevertheless lessons for the business community to apply to its response and recovery.

For those business leaders struggling to make sense of what's happening to their organizations and how to quell the damage—it's not too late to start making plans to facilitate your enterprise's move forward into recovery, all while vastly improving your IT operations.

There are four steps you can take today to help turn your good business into a great one, ready to weather the next crisis:

- Conduct a post-crisis assessment
- Create a future-state vision
- Enhance technology
- Define operational excellence

Conducting a post-crisis assessment

A first step to take post-crisis, or even sooner, as organizations look toward recovery, is to make an honest assessment of what worked, and what didn't, during this time. Remember that there is never a perfect solution for resiliency in a crisis—just degrees of success and failure. It's also useful to remember that no one alive today has direct experience with the effects of a pandemic on a national economy, so this is truly uncharted territory.

This assessment can help prepare for a future crisis and potentially even help eliminate related damage to the enterprise. In conducting this assessment, leaders should ask two key questions:

- What part of our IT operations did not work during the crisis?
- Where did we succeed?

What did not work

In the case of this pandemic, we know that most people—business leaders included—grossly underestimated the immediate severity of the contagion, the strictness of the infectious disease experts' and CDC's recommendations to contain its spread, and the state and federal governments' responses to those recommendations (many of which are still unfolding).

The crucial point here is to understand what, specifically, affected your company—and how. For example, in many organizations, staff are not permitted to access their office buildings, and some are not allowed to leave their homes altogether. System components in data centers may be going unrepaired and unreplaced and, consequently, some critical processing capabilities may be lost.

Many companies are also likely unprepared to support a predominantly remote workforce, so they may lack the infrastructure—such as enough VPNs— to support a remote working model. New security concerns can also affect organizations that suddenly have so much data distributed amongst so many remote workers.

What did work

Alternatively, companies that have been able to weather the COVID-19 crisis effectively have likely had enough VPNs to support a mass remote-work model, as well as a distributed security setup—such as multifactor authorization (MFA). These companies also most likely made investments in public clouds, helping to alleviate the pain of being unable to enter traditional data centers. In fact, cloud computing makes enterprises much less dependent upon those physical data centers, an advantage during shelter-in-place orders.

Creating a future-state vision

Once you've conducted a post-crisis assessment, the next step is to create a vision of your future state—that is, a vision of how you'll transform your technology in preparation for handling future crises more effectively. There are several activities that you should undertake to develop your future state. These include:

Determine the business priorities.

Agree on what issues are most important for the business, and then place them in ranked order. Keep in mind that everything can't be important. A trade-off must be made between what the business can afford—and truly needs—and what everyone thinks the business needs. These priorities will translate into a roadmap for any required transformation.

Determine the enabling technology.

Begin to put those technologies that will enable your transformation on your radar. These could include cloud-based systems, networking upgrades, and other things needed to make your systems more resilient during a crisis like a pandemic. Here's where your analysis of what worked, and didn't, during the COVID-19 crisis comes into play. Learning from experience and shoring up weaknesses by using whatever technology is appropriate for your organization is key—not just cloud.

Define success.

Create new metrics that will define a solution that meets the needs of the business. In other words, understand what success means to the business, what success looks like, and what changes will reflect this success. This process typically includes stress-testing, such as simulating a natural disaster, to understand how well your new technology configuration will perform under conditions as realistic as possible to a similar crisis.

Evaluate risk.

Evaluate how particular changes in technology will reduce or increase your risk. For example, how much are changes likely to cost? Or, what benefit(s) might a certain change provide—especially relative to its cost? This risk evaluation is essential for a couple of reasons. First, it's necessary to understand the business case, which requires placing a dollar amount on each benefit and each detriment. Second, it's also important to place a dollar amount on risk itself. For instance, not leveraging the right technologies could result in huge risk costs during a crisis.

Enhancing technology

Once your future state is defined and you've evaluated the potential risks involved, you can begin to migrate to the technology you've chosen to help mitigate your issues and improve your ability to work through a crisis. Migration typically involves a few core components—such as storage, compute, security, governance, applications, and data—as well as performing an evaluation of how your organization can move those components from a platform of higher risk to a platform of lower risk.

Keep an open mind. The answer is not always "the cloud." The purpose of planning the move is to develop a resource-migration strategy that conforms to existing business requirements. Remember, your migration will hardly be successful if critical systems crash while you're migrating to more resilient systems.

This step is also where you will determine the resources needed to migrate to your future state. The evaluation of those resources should include looking at people, tooling, platforms, funding, and outside assistance. Be careful to get this right! Most migration projects fail when the need for these resources is either under- or overestimated.

Once you've determined what migration resources you'll need, you can develop a timeline for migration—that is, what will move and when. One way to help make sure critical tasks are completed on time is to establish a project management office and look for, and resolve, dependencies that could hold up progress.

The final task in planning your migration is to develop metrics to measure success, and monitor them, to "prove" productivity and assure stakeholders that you can meet the expectations of the business. Because technology migrations are major investments, stakeholders typically require these assurances in writing.

Defining operational excellence

Once you've completed your migration planning, and as you move to the operational stage, you'll need to think differently about operational processes and tooling. Those companies that moved to cloud-based platforms pre-COVID-19 will most likely realize at this stage that they need a cloud operations (CloudOps) team with specialized tooling to manage public cloud-based platforms.

Other ops issues may include automating networking operations runbooks and implementing security operations (SecOps), as well as determining what other, additive processes are needed to support the new technologies you've put in place.

These new ops processes and the tooling should carry their weight by providing additional agility to existing systems. This includes the ability to:

- Move processing and storage from one geographical region to another, as needed
- Provide proactive security monitoring and automated responses
- Auto scale to more effectively utilize resources
- Provide self-healing capabilities, as well as links with management and monitoring systems for cloud and noncloud systems

Another objective in building operational excellence should be to strive for continuous improvement of operational systems. You can improve by constantly evaluating whether systems are optimized in the best way possible. If the answer is "no," then a microplan should be put in place to facilitate improvement. This constant evaluation helps you optimize cloud and noncloud operations and reflect the goal of customer and employee satisfaction in all your metrics.

Getting started

All of this might sound overwhelming, but overall, it's a simple pattern. Understanding what went wrong and what went right, and what needs to change, can help prevent the same things from going wrong again during a future crisis. Then, learn from the mistakes you made, because a mistake can often be the most valuable teacher and motivator.

Going forward, it's likely that much of what's outlined in this paper will be mandated by stakeholders at many companies as a way to help mitigate future risks, so if you start now, you'll likely be ahead of the competition. Remember: Future success isn't necessarily about the things that went wrong during a crisis like the current pandemic; things always go wrong. It's about learning lessons from mistakes so you can recover and thrive.

Let's talk

Dave Linthicum
Chief cloud strategy officer
Deloitte Consulting LLP
dlinthicum@deloitte.com

To find out more, please visit www.deloitte.com/us/cloud.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States, and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.