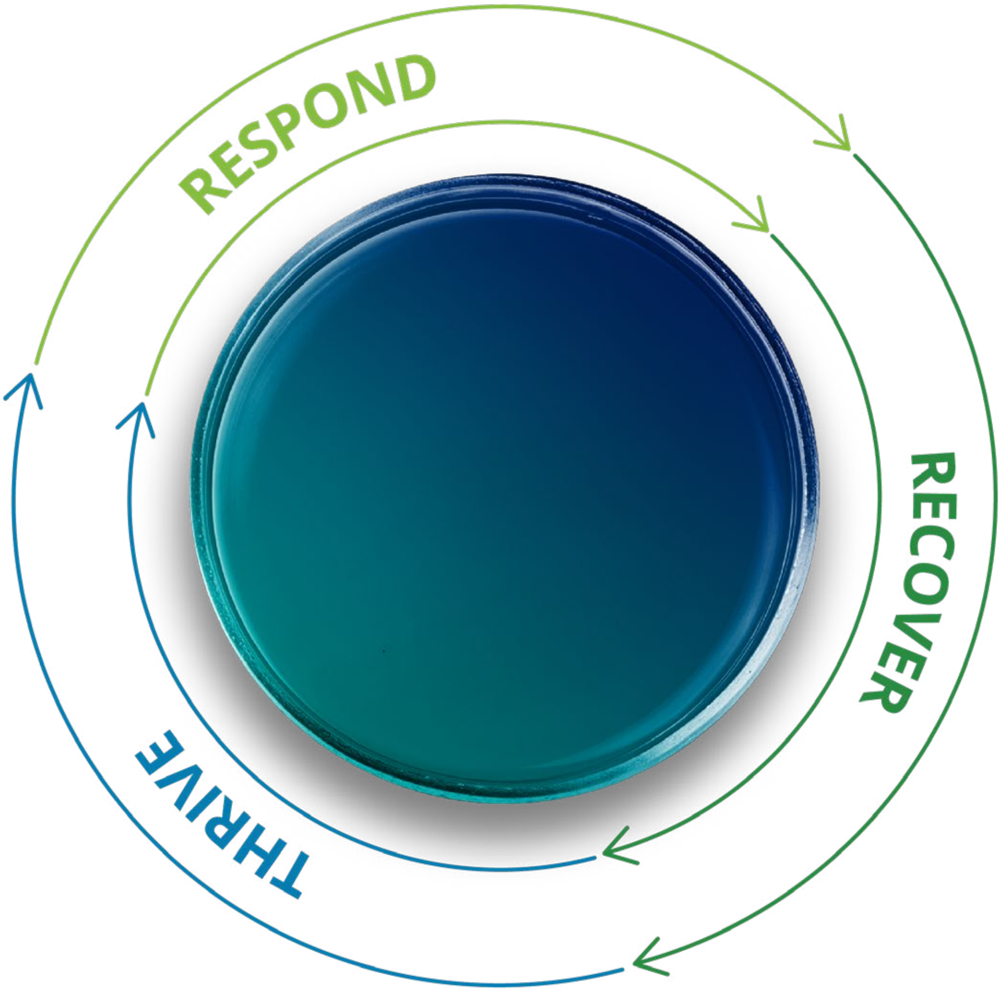
Deloitte.



Is your IT organization shaping tomorrow?

Navigating change: an unprecedented challenge.

None of us can predict the true impact of the pandemic on the global economy, but at this pivotal moment, there are clear choices to be made. A fundamental quality of **resilient leadership** that distinguish **successful CIOs** as they guide their enterprises through the COVID-19 crisis: Embrace the long view. Resilient leaders stay focused on the horizon, anticipating the new business models that are likely to emerge and sparking the innovations that will define tomorrow, the "next normal".

We believe that a typical crisis plays out over three time frames: **respond,** in which a company deals with the present situation and manages continuity; **recover**, during which a company learns and emerges stronger; and **thrive**, where the company prepares for and shapes the "next normal." Any period of volatility can **create opportunities** that businesses can leverage if they are prepared. As we have been adjusting ourselves to the new normal for several weeks now, this paper prepares CIOs to make the right decisions within the **recover** and **thrive** phase.

Public policy measures put in place to contain the spread of COVID-19 are resulting in **significant strategic and operational disruption** for many companies. In response, a majority of the workforce moved to remote work and therefore the ability to meet virtually is critical to move initiatives, projects and day-to-day work forward. To enable this way of working, companies need robust processes and **reliable technology solutions.**

This crisis forces IT organizations to reflect about the two opposing forces that are present in their company. On one hand, the need to digitalize their way of working: remote working, new ways to communicate with employees, clients or suppliers, cyber security, etc. On the other hand, IT is seen as a cost item and is often the victim of underinvestment or savings. These unpredictable times can be used as an opportunity by CIOs to get this paradox out of the way and guide their IT services and organization into the new tomorrow.

Following the global COVID-19 crisis, Deloitte has set out **9 key considerations** for CIOs to keep in mind to accelerate digital transformation initiatives and prepare the organization into the future.

1. IT Strategy

"Set out a clear goal and long term vision on how the post-COVID world will look like"

Organizations need strong leaders who define a clear way forward. More than ever, organizations need to think what digital transformation means for their organization and processes.

- How will business transactions be organized in the future?
- How can products be redesigned so they fit todays needs where social distancing will be the norm for quite some time.
- Where can IT help to reduce costs and make the organization stronger in the economic crises.

This makes that todays crisis serves as an ideal moment to revise the IT strategy and organization not only to cope with the economic risks of savings and social distancing restrictions but also to be stronger in the post-COVID time.

2. IT Operating model

"Create a flexible organization ready to cope with uncertainties, change and increased speeds of digital transformation "

In times of crisis, an important consideration is to think about what the impact will be on the IT operating model of the organization. Digitalization is fundamental to keep the business running. Some key considerations during this COVID-19 crisis are the following:

- Governance – keep the overview on the IT organization and adapt where necessary. Foresee new policies and procedures to clarify the new ways of working. Define goals for the recover and thrive phase.
- Re-evaluate escalation paths to effectively escalate and communicate.
- Critical roles– Define critical roles and functions and design backup plans for those roles and functions to guarantee continuity. (Refer to 9 – "Create a more resilient workforce").
- IT and operational processes – Identify key changes in processes and opportunities to automate processes (e.g. service desk functionalities) and ensure a smooth connection with the (digitalized) processes of clients and suppliers.
- Third parties – Evaluate collaboration with third parties. Which processes need to be ensured?
- Efficiency – Ensure efficiency in the internal working of the organization to create cost efficiency. Possible considerations are onshore and offshore working, removal of non-critical processes etc.

3. IT budget

"Develop a clear vision aligned to the changing priorities of your organization"

IT organizations often have multiple IT projects in flight at any given time in addition to normal business operations. Given the resource constraints and shifting priorities organizations may experience during this time, CIOs need to consider diverting people and technical resources to maintain critical business operations and projects for the future. Having a clear view of the prioritization and planning to stop or continue projects is important. In doing so, it is important to look at the entire project portfolio. Develop a clear vision within the organization on which projects resources need to be allocated.

With the increase in remote working, IT investments are necessary to provide a secure way of working for employees. Remote working entails several security risks that can disrupt continuity of the business. The lack of IT investments can impose severe security problems resulting in loss of sensitive data and loss of confidence from the consumer.

This digitalization can not only now, but also in the future, help organizations with improving its IT efficiency. The digital workspace can enable organizations to think about off- or nearshoring as a solution for cost and resource saving.

IT Investments during the pandemic crisis are not lost. Having secure and reliable IT systems that support critical business processes will benefit in the long run and prepare the organization for other crises that may hit us all.

4. Remote working

"Ensure (critical) resources/assets stay available and secure for working remotely"

As remote working has become the new normal, organizations have to ensure that they have the right policies and technological infrastructure in place to support this change in the way of working. In order to preserve the continuity of business operations we have listed some considerations below:

- Ensure compatibility between the organization's tools and those clients and suppliers are using.
- Keep the helpdesk running in case employees need support with their hardware or software. Provide live-support for the most critical problems.
- Continue monitoring the network for peak traffic demands and security breaches.
- Consider the purchase of additional licenses for collaboration tools such as Skype and Zoom.
- Even if VPN has been implemented, security should stay one of the top priorities.
- Avoid using open public tools like WeTransfer to transfer business sensitive data.

5. Business continuity

"Focus on ensuring organizational resilience by responding and recovering correctly"

The COVID-19 crisis has changed the organization's ways of working and organizations had to respond quickly to this new environment. Most of them shifted to a remote way of working and secured their most critical assets. The organizational strategies and plans they have put in place should ensure organizational resilience.

The first plans that are important have in place are the business continuity (BC) and disaster recovery (DR) plans. Assessing risks and their potential impact, developing recovery strategies, and having clear escalation procedures are all part of the BC plan. The DR plan focusses on how to get the technology environment back to normal.

In addition to the BC and DR plans, there are other important aspects that need to be taken into account:

- Revise the IT communication plan. Is the organization communicating with employees, customers and suppliers in a fast and effective manner?
- Perform scenario planning to understand the technology needs of the organization. Is the (IT) organization prepared to deal with the long term consequences and a new digital way of working?
- Plan for the recovery rebound. Consider in advance how to restart disrupted IT services.
  - E.g. Does the (IT) organization have the necessary tools in place to facilitate 'return to (the new) normal' (e.g. reservation tool for office spaces, etc.)
- Are the Single Points of Failure identified in the organization? Are there backups in place?
- Consider "lessons learned" from the previous weeks.
- Revise contingency plans concerning IT service providers and suppliers.

6. Relationship with customers

"Stay engaged with your customers and intercept the shift in their needs"

This is a critical moment that matters in the relationship with customers, and it is a time for the organizations' brand to lead. Customer needs can shift dramatically during crises such as this one, often from the rational to the emotional, and it is important for organizations to intercept that shift.

Establishing out-of-band communication channels can be a way to reach customers when regular channels are not available due to the crisis situation. Find and use alternative channels and online tools or applications to stay connected with clients. Being able to communicate and help customers during a crisis, will create a relationship that will last even when the pandemic is over.

The COVID-19 crisis can be an enabler for the organization to accelerate digitalization. Use it as an opportunity by setting up new platforms (e.g. virtual helpdesk, dashboards, chatbot, digital communication platform, ...) to communicate with external customers. IT-organizations or departments should also consider ways of digitizing communication with their internal customers. Implementing new ways of working together (e.g. implementation of Zoom for online meetings), poses new challenges for the organization. Is the network able to handle peak traffic? Are digital meeting rooms secure enough? Is there a helpdesk in place to support customers?

It is during a crisis like the one we are facing now, that opportunities rise for CIOs to prove the worth of IT projects, IT systems and IT services.

7. Vendors & suppliers

"Identify your critical vendors, partners and suppliers, evaluate your agreements but most important try to strengthen the partnership"

This COVID-19 crisis has an impact on the entire ecosystem of organizations. Identify critical technology vendors, partners and suppliers and confirm they are able to deal with spikes or adjustments in demands. Subcontractors may have less people at work because of illness or technical unemployment, this can result in waiting time for the organization. IT material can arrive later due to border closure. Take these risks into account while conducting a business impact assessment. Collapsing demand and supply chain shutdowns, e.g. not being able to deliver to customers due to lack of stock, can restrain cash and working capital of businesses, endangering the financial health of the company.

Re-discuss the terms of the Service Level Agreements (SLAs) with IT service providers, taking the impact of the current situation in mind. Prioritize services that are critical for the business and ensure that SLAs are adjusted and properly communicated.

8. Cyber Security

"Protect your IT organization to safeguard your networks and data"

A particular concern is that cyber risk multiplies when the workforce is suddenly distributed. Although many companies may be set up for remote work, far fewer have the proper cybersecurity protocols in place. Since the crisis began, phishing scams and other attacks have been on the rise, targeting employees working from home or from any other open network. Does the IT organization have the right protection in place to safeguard networks and data? Take the following guidelines into account to protect data and intellectual property:

- Remote working increases the use of personal devices for work. These devices may lack the latest security patches and tools to safeguard sensitive data.
- Develop corporate security policies and guidelines concerning the use of personal devices.

- Make sure digital capabilities are tested and ready to be scaled (e.g. increased usage of VPN).
- Cloud based communication platforms may allow third parties to access sensitive information.
- Assessing cyber governance and security awareness in the new (remote) operating environment.
- Implement authentication and access control mechanisms to ensure secure connections.

9. Talent

"Create a more resilient workforce"

Organizations might face a rise in absenteeism as health-screening protocols are enforced and people who have symptoms are quarantined. Ensure business continuity plans take these labor shortages into account and prepare succession plans for key positions in the (IT)-organization.

The current situation may also present an opportunity to think about how CIOs can elevate communication, create a more resilient workforce and build more focus on health and well-being. Invest in training employees to have an answer to the new needs, these skills are not lost and can be an added value for the organization after the crisis.

Organizations should take near- or offshoring into account when thinking about a resilient workforce. These options can be cost effective options to counter a drop in productivity during this crisis due to for example illness of employees, but will also enable organizations to handle the increase in demand after this period.

To ensure business continuity and the safety of employees after this pandemic crisis, organizations should consider implementing safeguards:

- Divide the workforce in A and B teams to avoid contamination of all employees. If one team falls ill, the second team can continue the critical business processes.
- Formulate a backup plan for critical employees. E.g. does the organization have a backup network engineer in case he is absent for a long period in time?
- Train employees to work with the new tools and new ways of working, this both on a user level as on admin or development level.

Prepare for the new tomorrow

Many technology leaders today are in a unique position to help their organizations reimagine the future of work, of the workforce, and of the workplace powered by technology. We are at an inflection point where technological capabilities are ready to transform every facet of work as we know it. Now is the time for CIOs to highlight the positive effects that a digital transformation can have for the organization. Ensuring business continuity, providing security, enabling more cost effective ways of working, ... All this can happen by implementing new tools like automation, robotics or cloud in the organization. The key is to enable present workarounds and use this as an opportunity to shape the future ways of working, which are more efficient, effective and collaborative, beyond the boundaries of the function and the enterprise. Use this time as an opportunity to accelerate digitalization to the future of work.

Contacts

Michel De Ridder
Partner Technology and digital risk
mideridder@deloitte.com
+ 32 2 800 24 14

Chantal Mons
Director Technology and digital risk
cmons@deloitte.com
+ 32 2 302 25 90

Julie Van der Planken
Director Technology and digital risk
jvanderplanken@deloitte.com
+ 32 2 800 27 09

Johan Van Grieken
Partner Technology and digital risk
jovangrieken@deloitte.com
+ 32 2 800 24 53

Koen Magnus
Crisis & Resilience leader
kmagnus@deloitte.com
+ 32 2 800 24 43