

Cloud, networks, and modern infrastructure in the wake of COVID-19

From crisis response to thriving in the new environment



Real insights

The road through recovery and emergence into the new reality is rewriting the world as we know it. The technology shift that we thought was five years out is now expected to happen over the next two years. While different industries and markets will follow different paths and speeds into this uncharted future, all will exist in a much more digitally connected world.

Critically important is how the digital backbone of a hyper-connected world (devices, cloud, network, and modern IT infrastructure) underpins your ability to deliver this change. These three main areas include:

1. Remote at scale
2. Cost-optimized delivery
3. Resilient agility



Triggers and pain points

- Remote collaboration and working tools insufficient for the users' needs
- Inability to dynamically scale system capacity and network bandwidth to maintain a positive customer experience
- Slow turnaround times to provision foundational infrastructure components (servers, databases, security, monitoring, etc.)
- Inability to quickly pinpoint and resolve performance issues
- Unclear hybrid, multicloud, and workload placement strategies
- Limited visibility into cloud and infrastructure usage and spend
- Stale resiliency and disaster recovery plans and architectures for critical system infrastructure and network segments
- Vendor lock-in hindering ability to quickly pivot and deliver expected features and functions at speed

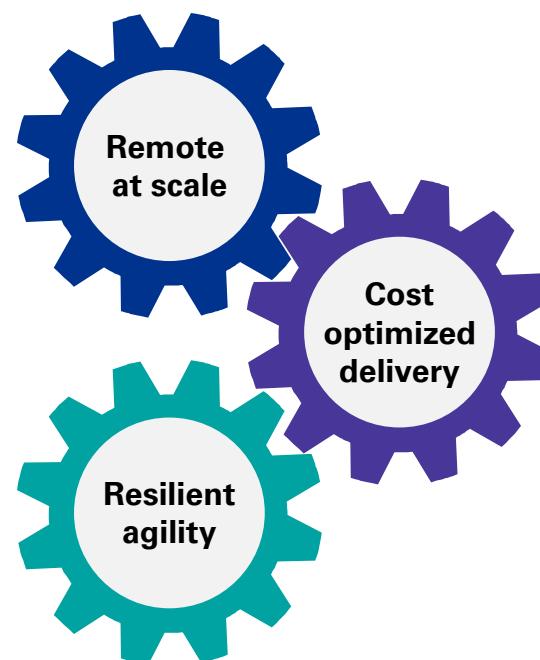


Our perspective

Many organizations have quickly deployed additional digital capabilities to keep business running and employees and customers connected. As the new reality emerges, organizations will need to continue to build a digital backbone using cloud-native solutions, anywhere connectivity, hybrid multicloud architectures, and an automated and secure delivery chain with the speed and flexibility to meet rapidly evolving business needs.

Our recent client discussions have validated three focus areas that technology executives should consider:

1. Remote at scale – Shift the mindset to work from anywhere:
"We quickly realized there were many physical and manual steps in our processes so we needed to quickly ramp up automated online workflow and e-signature capabilities."
2. Cost-optimized delivery – Build a hybrid cloud environment to flex capacity where needed:
"Segments of our business ramped down production while others were ramping up, but it was extremely difficult to migrate unused infrastructure capacity from one area to another."
3. Resilient agility – Embed security, performance, and resiliency in the infrastructure stacks:
"The crisis has highlighted the need to quickly determine the health to prevent downtime of systems serving our customers in their time of need."



	Resilience	Recovery	New reality
Remote at scale	<ul style="list-style-type: none"> – Identify critical application infrastructure components and specific impacts – Prioritize requests to keep the organization connected and working – Enable remote monitoring and management of IT estate – Update risk and performance indicators 	<ul style="list-style-type: none"> – Evaluate IT capabilities to meet evolving experiences and operational needs – Proactively shift the operating model to effectively manage the network and hybrid cloud environments – Continually monitor and adjust infrastructure capacity and performance 	<ul style="list-style-type: none"> – Align user collaboration and productivity improvement to infrastructure and network updates – Determine hybrid, multi-cloud solutions suitable to deliver a sustainable “work from anywhere” paradigm – Review, challenge, and quantify critical infrastructure portfolios and contracts
Cost-optimized delivery	<ul style="list-style-type: none"> – Review infrastructure capacity needs – Communicate cloud strategy and guardrails – Remove manual handoffs and approvals – Adjust policies and IT operations practices – Focus on infrastructure performance 	<ul style="list-style-type: none"> – Model infrastructure capacity required to respond to the current situation – Reclaim unused and under-utilized infrastructure capacity – Automate tasks to reduce turnaround times – Update hybrid, multicloud usage and spend policies and guardrails 	<ul style="list-style-type: none"> – Accelerate the build out of the digital backbone using cloud native options – Systematically right-size capacity based on the current business needs – Automate an end-to-end delivery chain – Establish full stack operational and financial intelligence monitoring
Resilient agility	<ul style="list-style-type: none"> – Determine how to shift or burst workloads between on-premises and cloud environments – Update processes to quickly resolve issues and fulfill requests – Adjust risk and performance baselines for infrastructure components – Close resiliency gaps to meet RPOs and RTOs 	<ul style="list-style-type: none"> – Review infrastructure RPOs and RTOs – Update cloud provider preferences – Create hybrid cloud resiliency patterns and best practices – Update IT operational and cyber risk measures and indicators – Test resiliency plans and solutions 	<ul style="list-style-type: none"> – Conduct BIAs and update resiliency strategies and solutions – Develop resiliency strategy and governance program – Shift to a hybrid, multicloud strategy – Establish infrastructure stability and reliability measures

Throughout this document, “we”, “KPMG”, “us” and “our” refer to the network of independent member firms operating under the KPMG name and affiliated with KPMG International or to one or more of these firms or to KPMG International.

©2020 KPMG International Cooperative (“KPMG International”), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.



Where am I now? - Qualifying questions

Resilience	Recovery	New reality
<ul style="list-style-type: none"> — Have you accounted for your cloud, infrastructure, and network spend? — Have you mapped applications and data to the underlying infrastructure environments? — Do you have a cloud strategy and capabilities for moving to and operating workloads in public cloud environments? — How are you addressing infrastructure and network capacity demands? — Can you scale to public cloud environments if needed? — Have you identified infrastructure components most impacted by COVID-19? — How are you capturing and managing infrastructure and network events, incidents, requests, and changes? — Do you have Disaster Recovery plans in place for critical systems? 	<ul style="list-style-type: none"> — Have you right-sized and or spun-down extra compute, storage, and network capacity? — Have you established best practices and policies for using public cloud and spend going forward? — What updates are needed to improve service management capabilities going forward? — What infrastructure-as-code patterns, templates, and repositories are in place? — How do you manage the use of cloud native architectures and capabilities across the organization? — Are you identifying and filling capability gaps in the architecture and delivery chains? — Are you working with your security and risk teams to embed policies and controls in to the architecture through “policy as code”? 	<ul style="list-style-type: none"> — How do you design the digital backbone to provide a seamless work-from-anywhere user experience? — How will you manage model infrastructure capacity plans for an uncertain future? — Does your cloud strategy address the right mix of providers, services, and platforms? — What are the objectives, results and service indicators for your infrastructure environments? — What cloud native tools and capabilities are needed to deliver value and outcomes? — How will you integrate capabilities into an automated end-to-end delivery chain? — Are you testing resiliency strategies and solutions? — How are tracking and testing change impact in an increasingly complex infrastructure environment?



Getting started

As with any journey, the biggest challenge can be taking that first step. Organizations can take the following actions to get started:

- Conduct business impact assessments to identify critical applications and map to underlying infrastructure and network components
- Determine additional infrastructure and network capabilities and solutions needed to keep the business running and users productive
- Determine infrastructure and network capacity, security, performance, and resiliency requirements to foster a positive remote working experience
- Work with organization’s leadership to set priorities for engineering and operating critical infrastructure and network components
- Develop a hybrid, multicloud strategy, including cloud native capabilities, starting with vision, guiding principles, and architecture design principles
- Update service management processes (incident, change, request, event) to address infrastructure changes due to the current situation
- Define objectives, results, and service indicators to communicate performance and value of the infrastructure and network environments
- Define and implement cloud spend optimization policies and procedures
- Identify delivery chain capabilities and tools, and start to establish an end-to-end delivery chain to automate activities, procedures, and processes

Contact us

If at any time you need help, please use the information below to get connected to a professional for more advice and support.



Steve Bates
Global Leader
CIO Center of Excellence
KPMG International
T: +1 303 295 5524
E: sjbates@kpmg.com



Priya Emmanuel
Managing Director
CIO Advisory
KPMG in the US
T: +1 312 665 3052
E: pemmanuel@kpmg.com



Craig Hays
Managing Director
Digital Lighthouse
KPMG in the US
T: +1 214 850 6832
E: craighays@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities

Throughout this document, “we”, “KPMG”, “us” and “our” refer to the network of independent member firms operating under the KPMG name and affiliated with KPMG International or to one or more of these firms or to KPMG International.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

©2020 KPMG International Cooperative (“KPMG International”), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved. Designed by CREATE | CRT126027

The KPMG name and logo are registered trademarks or trademarks of KPMG International.