RingCentral

# Understanding business continuity

# Understanding business continuity

If there's one thing the last few years have shown, it's that disasters can strike at any moment. The COVID-19 pandemic was a harsh lesson that despite even the best strategies, "business as usual" can be upended in an instant. And pandemics aren't the only disruptions businesses might face. From on-site emergencies to natural disasters and economic downturns, there's no shortage of disruptive events.

But preparation is the key to a speedy recovery. Though it might not be possible to predict a crisis, businesses can—and should—always plan for the unexpected. This means choosing the right cloud communications provider for the tools your business needs.

Think back to the earliest days of the pandemic when the lockdowns began. Some organizations—namely enterprises and large companies—were well-positioned to transition to remote work and continue collaborating. Others weren't so prepared, forcing them to rush the deployment of ad hoc solutions and processes that weren't as effective.

**Business continuity** is the preparation for this sort of sudden, unexpected upheaval. A business continuity plan encompasses all of the strategies that must be put in place to mitigate any type of crisis, with well-defined and tested tools and processes ready to go.

For example, if one of your business's locations was flattened by a natural disaster, how would the employees who worked there continue working? Will they have the right tools? How quickly can your business restore its critical functions? A business continuity plan addresses those issues while maintaining a service level.

# How your service providers play a role

A well-designed business continuity plan requires you to evaluate the strength of not just your technologies *but the service providers behind them too.*

Take communications for example. Employees depend on their communications tools to work together every day. What happens in the event of a crisis? Will your service provider remain online? Will they enable your employees to continue collaborating, regardless of where they are? How can they guarantee that for you?

In other words, a big part of your business continuity plan rests on your communications provider. And how resilient they are in the event of a crisis will depend on three core factors: *infrastructure, mobility,* and *global continuity.*

The next few pages will show you how to evaluate your providers for business continuity.

# Evaluating infrastructure

It's easy to assume that your tools will stay online in the event of a crisis. After all, your communications live in the cloud, where they're immune from outside forces, right?

Well, that all depends on your provider. Cloud infrastructures live in data centers managed by your provider's on-site personnel. While that means your communications are safe from events within your organization, outside forces (such as pandemics) could affect your provider. How their infrastructure is built will impact your business continuity plan.

Use the following to assess your communications service provider:

**What to ask:** How does the service provider's infrastructure stay online in the event of a disaster?

**What to look for:** Cloud service providers are subject to the same risks as businesses—events such as fires, hurricanes, and other disasters can all wreak havoc on their systems too. However, it's the role of a dedicated service provider to ensure that their infrastructure has appropriate redundancies built in, so that if a problem occurs on their end, your business will not be affected.

An important way providers can guard against localized risks is to house their infrastructure in multiple geographically distributed data centers—for example, on both the east and west coasts of North America. This distributed strategy reduces the risk of service interruptions due to a natural disaster by quickly routing the service to another data center location when one data center is affected.

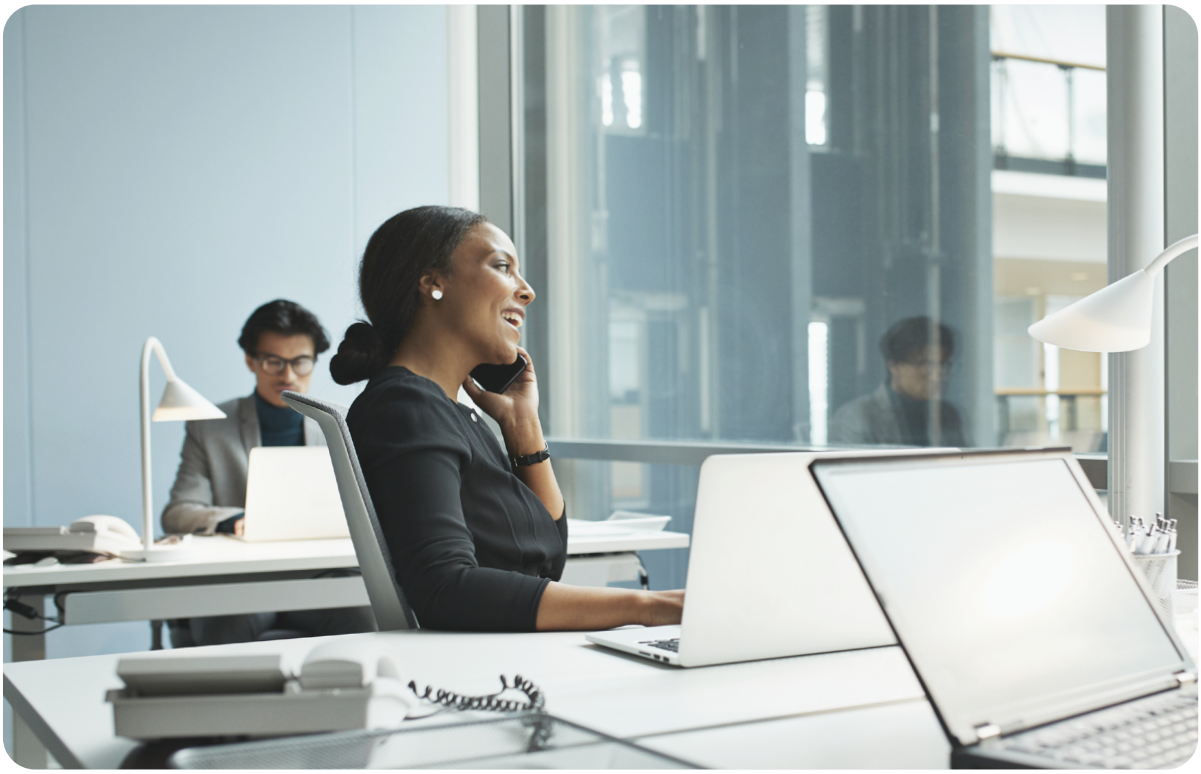
Your provider should have built-in architectural redundancies as well. This includes multiple internet transits, backup power supplies, a backbone of connectivity built upon multiple top tier global telecommunications providers, and standard practices of securely replicating data across data centers.

Combined, these redundancies ensure that if a failure is detected, your provider can easily re-route to other data centers. Even in the face of a catastrophic localized event, your communications experience no interruption of service.

**What to ask:** Does the service provider have documented practices and policies to address outages?

**What to look for:** Your cloud communications provider should have up-to-date, regularly tested procedures ready to implement in case of an outage on their end. Such plans should be fully transparent so that you can compare providers' approaches and feel fully confident in your provider's ability to maintain service in the face of any issues.

A disruption or outage is exactly when the redundancies outlined above kick into place. First, your provider should have robust 24/7 monitoring in place to immediately identify any issues within its network. Your provider should also be able to tell you how, in the event of a failure, they can ensure a rapid transition to a backup system, whether within the same data center or one at another location. Armed with this information, you can assess how well equipped your provider is to keep your business connected in the face of an issue.



# Evaluating mobility

An unexpected event can completely disrupt a company's workflow—including how and where employees are able to do their jobs. Additionally, companies are increasingly moving towards hybrid work models, where employees split their time between the office and home.

That's why businesses should ensure that even when employees aren't in the office, they can still perform their jobs normally. Here are a few questions to ask about this topic:

**What to ask:** How will the service provider support your mobile or remote workforce in the event of a disaster?

**What to look for:** In the event of a disaster, workers might not have access to their offices at all—and possibly for a prolonged period. If this happens, the ability to deploy communications services to anywhere employees need is critical to maintaining operations.

For cloud communications solutions, this mobility is a built-in advantage. A cloud-based system can securely deploy messaging, video, and phone capabilities over the internet to any device—desktop, laptop, or mobile app. For optimal mobility, communications should also work on any type of connection: Wi-Fi, 3G, 4G, and 5G. This makes the entire system portable.

Additionally, look for a provider that offers an app version of their platform. Workers can use the app—in lieu of a PC—to access the same functions as they would on their PCs. They can collaborate with peers, fulfill customer service queries, and perform other tasks just as easily as if they would in the office.

**What to ask:** Does the service provider offer a mobile app? Can it perform as well as the desktop app?

**What to look for:** In many cases, your employees won't always have access to their PCs, especially those who work exclusively on-site. That leaves them without a means to communicate until the emergency goes away or the company distributes laptops to employees' homes.

Look for a provider who treats its mobile users as first-class citizens—on the same level as its desktop users. Ideally, the mobile app should offer access to most, if not all, features available on the desktop version—namely messaging, video conferencing, and phone. That way, in emergency situations, employees can still communicate and collaborate with their teams.

**What to ask:** Does the service provider offer multiple modes of communications so that if one is affected, other modes can be used?

**What to look for:** Ideally, your cloud communications solution has multiple modes of communications, including team messaging, video conferencing, calling, SMS, fax, and more. Since each of these modes uses different network architectures for delivery, your users are guaranteed to have as many bases covered at all times.

**What to ask:** How will users access their communications?

**What to look for:** Employees will need their communications regardless of where they are. If employees have a stable internet connection, they should have access to every feature available to them, whether on PC or mobile. Login features—such as multi-factor authentication—should be built into the product so that employees can easily and securely sign in to their communications from anywhere in the world.

**What to ask:** What if my internet goes down while working in the office?

**What to look for:** When it comes to cloud technologies, an internet outage can leave companies without access to their communications. But you're not always out of options.

Look for providers with solutions that can deliver certain services despite internet outages in your offices. Your provider should be able to deliver certain essential services, including:

- Emergency calls
- Outbound and inbound calls
- Extension-to-extension dialing

Your communications applications should run on both Wi-Fi and 3G/4G/5G, keeping your users connected in any network environment. Users should also be able to make calls using their mobile phones' native cellular networks while still maintaining their business caller IDs.

**What to ask:** Does the cloud communications provider support emergency 911 access? How are e911 requirements met for a distributed workforce?

**What to look for:** Accessing emergency services can be more complicated with a cloud-based communications system. For example, 911 can easily trace the originating address of a call made from a hardwired phone, while cloud solutions often require phone numbers to register a corresponding address. If the most up-to-date location information is absent, there can be dangerous confusion and delays in reaching fire departments, police, or first responders.

Look for a provider that makes it easy to keep this critical data up to date, even during periods of disruption. For users on the corporate internet network, the cloud communications system should be automatically able to recognize the location using Wi-Fi access points. But when a user logs into an off-site network, the system should immediately prompt them to update their location.

# Evaluating global business continuity

One way businesses have changed over the last few decades is that many have expanded their global footprints, opening new offices, branches, plants, and other satellites in new countries.

These networks create business opportunities, and they can help to build redundancy into the corporate structure. This can be a boon for business continuity—but only if you're working with a global provider that can help your organization leverage its expanded workforce in a crunch.

**What to ask:** What is the service provider's commitment to global system availability?

**What to look for:** Businesses that depend on local solutions are at the mercy of regional forces. Things like the reliability of local telecom providers—which may vary regionally—and natural events can put some markets at greater risk of service interruptions.

However, providers are typically able to guarantee a specific level of service availability that accounts for both planned and unplanned disruptions. This guarantee comes in the form of a service level agreement (SLA), which promises uptime in a percentage form. For example, an SLA of 99% guarantees no more than 1% downtime—or 7.2 hours of downtime per month. An SLA of 99.999%—considered the gold standard—translates into just 26 seconds of monthly downtime.

Look for providers that have the distributed geographical capabilities to work around regional issues. For example, providers with geo-redundant data centers can rely on their global network to offer 99.999% uptime, making critical capabilities such as voice available at all times.

**What to ask:** Can we make emergency changes to the communications system (such as the rerouting of functions)?

**What to look for:** A localized disaster can prevent employees within an affected market from immediately resuming operations. In order to ensure business continuity, a global organization may then want to reroute some functions to employees in another market until normal operations can resume.

Shifting work to unaffected markets can be relatively simple if all locations are already employing the same communication tools and your solution allows you to make remote, on-the-fly changes.

Look for a provider that offers a centralized administrative portal that allows for off-site system management. Being able to make changes remotely via a web-based, centralized admin site will allow your business to easily reassign and reroute calls and workflows to a market that hasn't been impacted.

# Other business continuity requirements to consider

Disasters can cause a lot of confusion in an organization—and when it comes to your communications, being kept in the dark can be catastrophic. You'll need to look for a provider that's committed to transparency and communicates at the first sign of disruption.

**What to ask:** How will the provider keep customers informed at every step of the way?

**What to look for:** When a problem occurs, your service provider should act as a partner, not a hindrance. This means they should have a plan to proactively communicate status updates and other information regarding an outage to its customers, employees, third-party providers, and local governments, as needed.

This commitment to proactive and reliable communication should be baked into your provider's own business continuity plan. They should be able to outline exactly when and how they will communicate in the event of an issue, including details such as what the issue was and how it was resolved.

**What to ask:** Does the provider offer other ways to stay in the know?

**What to look for:** Ideally, you'll want to work with a provider that maintains an updated site for customers to see all known system issues that could impact their service, preferably with drill-down capabilities to see the status of the network node where your account resides. This service portal should help confirm whether there are outages, that endpoints are configured properly, and that environments meet network requirements and recommendations.

# About RingCentral

RingCentral, Inc. (NYSE: RNG) is a leading provider of business cloud communications and contact center solutions based on its powerful Message Video Phone™ (MVP™) global platform. More flexible and cost effective than legacy on-premises PBX and video conferencing systems that it replaces, RingCentral empowers modern mobile and distributed workforces to communicate, collaborate, and connect via any mode, any device, and any location. RingCentral offers three key products in its portfolio including RingCentral MVP™, a unified communications as a service (UCaaS) platform including team messaging, video meetings, and a cloud phone system; RingCentral Video®, the company's video meetings solution with team messaging that enables Smart Video Meetings™; and RingCentral cloud Contact Center solutions. RingCentral's open platform integrates with leading third-party business applications and enables customers to easily customize business workflows. RingCentral is headquartered in Belmont, California, and has offices around the world.

For more information, please contact a sales representative.
Visit ringcentral.com or call 877-596-2939.

RingCentral

776232652 10/2021

RingCentral, Inc. 20 Davis Drive, Belmont, CA 94002. ringcentral.com