Gartner Research

5 Actions to Manage Outsourced Service Impacts Due to Coronavirus and COVID-19

David Groombridge, VP Analyst
Brett Sparks, Sr Director Analyst
Stephanie Stoudt-Hansen, Sr Director Analyst

19 March 2020

Gartner

5 Actions to Manage Outsourced Service Impacts Due to Coronavirus and COVID-19

Published 19 March 2020 - ID G00722531 - 32 min read

By Analysts David Groombridge, Brett Sparks, Stephanie Stoudt-Hansen

Initiatives:IT Services and Solutions

The rapid spread of the coronavirus (the virus that causes COVID-19) across many countries has the potential to affect the delivery of outsourced IT services. Sourcing, procurement and vendor management leaders must act immediately through five key actions to minimize the impact to their businesses.

Overview

Impacts

- With multiple providers impacted globally by coronavirus (the virus that causes COVID-19), sourcing, procurement and vendor management teams may struggle to prioritize where to focus immediate risk mitigation actions.
- Service providers may struggle to meet contractual service obligations due to large-scale staff absences or inability to work from an office environment. Most contracts provide little protection due to the force majeure nature of a pandemic.
- Global and national contingency operations to prevent the spread of the virus may well create longer-term changes in the economic outlook, requiring service costs to be re-examined.

Recommendations

Sourcing, procurement and vendor management leaders responsible for outsourced IT services and solutions should:

- Prioritize outsourced services for risk mitigation by promptly analyzing the criticality of each service in your portfolio in a pandemic scenario and the likely change in demand for each service. Create an empowered team to enable rapid decision making during the crisis.
- Increase organizational resilience immediately by rapidly expanding remote working solutions for in-house and outsourced staff. Work with business, IT and provider teams to quickly deploy remote working technologies, increase available bandwidth and revise security approaches.
- Collaborate with providers to identify and close gaps in their business continuity and third-party risk plans by scaling back operations, stopping or delaying projects, optimizing delivery locations, temporarily relaxing SLAs, and changing shift patterns.

- Implement service-specific contingency plans for each critical service, by reducing low-priority demand, reallocating resources between tasks, increasing temporary crowdsourcing and insourcing, and utilizing alternate delivery methods such as online conferencing and automation.
- Plan for potential longer-term cost reductions resulting from the economic impacts of the coronavirus by preparing a list of potential cost optimizations by service line, with the time frames to achieve benefit.

Analysis

Organizations of all scales now take advantage of globalized service delivery offerings to optimize costs, buying a diverse range of outsourced services from providers in multiple countries. However, the advent of any event that creates international impacts will cause disruption to this global supply chain, and the coronavirus (the virus that causes COVID-19) seems likely to be the first such event to hit IT services globally.

On 11 March 2020, the World Health Organization (WHO) declared the COVID-19 outbreak a pandemic. [1] At that point, multiple countries were already impacted by outbreaks of the virus, with China, Italy, South Korea and Iran strongly affected and varying degrees of infections in many other countries. With a very rapid rate of spread, the coronavirus has the potential to create very high levels of staff absence for service providers. With further complications arising from governmental imposition of travel restrictions, shortages of supplies and reduced cash flows, service providers may struggle to deliver services to contracted levels. Further, contractual protections may be of limited use to buyers, as most providers' business continuity (BC) plans have been designed to deal with loss of a single site, rather than impacts across multiple countries. In addition, a global pandemic may well give providers the ability to exercise force majeure provisions in contracts (see Note 1). Indeed, the impact of the pandemic has already led to China issuing certificates of force majeure to its exporters, potentially allowing them to break contractual commitments. [2] Moreover, as the virus spreads unevenly across the globe, service and economic impacts may extend throughout 2020 and well into 2021.

In such a situation, sourcing, procurement and vendor management (SPVM) leaders are asking Gartner how to mitigate the impact of this pandemic in their major outsourcing deals. In this research note, we provide five key steps to use in collaboration with providers to minimize the impact to your organization's business operations.

Impacts and Top Recommendations for SPVM Leaders

Impacts	Top Recommendations
With multiple providers impacted globally by the coronavirus and COVID-19, sourcing, procurement and vendor management teams may struggle to prioritize where to focus immediate risk mitigation actions.	• Prioritize outsourced services for risk mitigation by promptly analyzing the criticality of each service in your portfolio in a pandemic scenario and the likely change in demand for each service. • Increase organizational resilience immediately by rapidly expanding remote working solutions for in-house and outsourced staff.
Service providers may struggle to meet contractual service obligations due to large-scale staff absences or inability to work from an office environment. Most contracts provide little protection due to force majeure.	• Collaborate with providers to identify and close gaps in BC and third-party risk plans by scaling back operations and services. • Implement service-specific contingency plans for each critical service by reducing low-priority demand, reallocating resources between tasks, increasing temporary crowdsourcing and insourcing, and utilizing alternate delivery methods.
Global and national contingency operations to prevent the spread of the virus may create longer-term changes in the economic outlook, requiring service costs to be re-examined.	• Plan for potential longer-term cost reductions resulting from the economic impacts of the virus by listing potential cost optimizations by service line, with the time frames to achieve benefit.

Source: Gartner (March 2020)

722531_C

Figure 1. Impacts and Top Recommendations for SPVM Leaders

Impacts and Recommendations

Immediate Priorities

Businesses of all scales are scrambling to provide mitigation of pandemic impacts. The first priority for any SPVM leader during the global pandemic is to act rapidly. Italy showed its first case of coronavirus on 30 January 2020, and less than 40 days later, its government introduced countrywide movement restrictions and a ban on public gatherings. [3]

Responses to the COVID-19 global pandemic cannot wait and cannot be delayed. The rapid rate of spread of the disease requires SPVM leaders to respond immediately, before services are subject to impact. The strategy should be: If in doubt, MITIGATE.

SPVM teams must rapidly identify the priority services for risk mitigation activity using Action 1, and work with providers to immediately expand remote-working capabilities using Action 2.

Action 1: Prioritize Outsourced Services for Risk Mitigation

The first step for any SPVM team has to be to prioritize which services to apply mitigations to, since the short response time available is unlikely to allow all services to be effectively mitigated.

The starting point for this has to be immediate engagement with the organization's business continuity management (BCM) team. Ideally, as part of previous business continuity (BC) planning within vendor management, the organization will already have identified its critical providers through a business impact analysis (BIA); if so, go directly to Action 2 below. (For more details, see the process set out in "Develop Contingency Plans for Your Critical Suppliers, or Risk Business Disruption" or how to derive a BIA in "The Business Impact Analysis: A Digital Business Essential.")

If identification of critical providers has not been done, though, Figure 2 provides a simple approach to rapidly identifying priorities. It is based on a hypothetical example showing likely location risks, anticipated demand and the relationship between functional outsourcing deals and critical business processes.

Prioritization of Outsourced Services to Mitigate Based on Business-Criticality of Processes and Location Risk

Outsourced Service	Key Service Locations	Alignment To Critical Processes				Service Impact Assessment			Overall Priority[c]
		CRM	Manufacturing	Billing	Process Alignment[a]	Current Location Risk	Expected Change in Demand	Service Impact[b]	
Finance BPO	Manila, Philippines	**2** — Medium	**3** — High	**3** — High	8	**2** — Medium	**2** — Stable	4	32
HR BPO	Prague, Czech Republic	**2** — Medium	**1** — Low	**1** — Low	4	**2** — Medium	**1** — Reduced	2	8
Application Development	Milan, Italy	**1** — Low	**1** — Low	**1** — Low	3	**3** — High	**1** — Reduced	3	9
Application Management	San Jose, Costa Rica	**2** — Medium	**3** — High	**2** — Medium	7	**1** — Low	**2** — Stable	2	14
Network Operations	Manila, Philippines	**3** — High	**3** — High	**1** — Low	7	**2** — Medium	**3** — Increased	6	42
Data Center Outsourcing	Pune, India	**3** — High	**3** — High	**2** — Medium	8	**1** — Low	**2** — Stable	2	16
End-User Support	New York, U.S.	**1** — Low	**1** — Low	**3** — High	5	**1** — Low	**3** — Increased	3	15
Service Desk	Bangalore, India	**1** — Low	**1** — Low	**1** — Low	3	**1** — Low	**3** — Increased	3	9
Security Services	Seattle, U.S.	**2** — Medium	**2** — Medium	**1** — Low	5	**2** — Medium	**3** — Increased	6	30

Source: Gartner

[a] Overall Sum of Scores

[b] Location Risk x Change in Demand

[c] Process Alignment x Service Impact

722531_C

Figure 2. Prioritization of Outsourced Services to Mitigate Based on Business-Criticality of Processes and Location Risk

Note: Location risk scores are for indicative purposes only.

SPVM leaders should use the prioritization matrix in Figure 2 in conjunction with business and IT teams. The required steps are:

- List all the services that the organization outsources to third parties, together with the location(s) from which each service is delivered.
- Next, list each critical business process identified by the BCM team. Identify the dependency of each process on each outsourced service, using a scale of 3 for high dependency, 2 for medium and 1 for low dependency (or a more granular approach). The alignment of each service to critical business processes is the sum of these alignment scores.
- For each location, assess the current risk of the coronavirus affecting operations in that service location. The table above uses a score of 3 for high risk, 2 for medium and 1 for low risk, but more granular scoring could be used. This scoring should also allow for potential mitigations for each location. Such mitigations could include the provider's ability to shift key services from a highly impacted to a less-impacted location, or the degree of automation applied at each location. For example, consider reducing the score if the service is more than 50% automated.
- For each service, assess the anticipated change in demand for that service during the period that business disruption will continue. Use a score of 1 if the service demand will be substantially reduced in the period, 2 if it will remain stable and 3 if it will increase. (The main example of increased demand is likely to be in networking or remote-working services, for example — see next section.)
- The overall service impact is then calculated by multiplying the average score for location risk by the expected change in demand as a result of a business disruption. In other words, service impact score = location risk score x change in demand score.
- Finally, prioritize services to mitigate by multiplying the scores for process alignment score and service impact (that is, overall priority score = process alignment score x service impact score) and identifying services with the highest scores as starting points. In Figure 2, network operations will be the immediate priority, with finance BPO and security services also as high priorities.

Other considerations may need to be factored into this assessment, such as whether a low-priority service has key personnel within it who need special prioritization in the assessment. Note that a prioritization of the type in Figure 2 cannot be a one-off exercise. It will need to be a living and versioned assessment, updated as business priorities change and the risk of COVID-19 in a given location changes. Multiple websites provide information on the spread of the coronavirus, [4] and these should be monitored daily for new information. Given the current speed of spread of the coronavirus, this may well be an assessment that has to be done daily. Allowing a rapid response

to changes in the prioritization will require SPVM leaders to delegate appropriate decision making to vendor managers and others dealing with providers and deciding on mitigations.

Action 2: Increase Remote-Working Capabilities

Gartner recommends remote working as a key element of CIOs' BC planning for the coronavirus (see "Coronavirus (COVID-19) Outbreak: Short- and Long-Term Actions for CIOs"). As organizations seek to mitigate the risks of the coronavirus in the workplace, many of them are likely to require more employees to work remotely for more of the time. [5] As a result, SPVM leaders must prioritize risk mitigation for services allowing such remote working, regardless of any other service prioritization resulting from Table 1 or elsewhere. This will require a range of considerations:

- **Network Bandwidth** — Sufficient network capacity is the key requirement for working remotely, so SPVM teams must prioritize this. Work with network providers to increase bandwidth, ideally on a burstable basis, but increasing fixed capacity if necessary. Work with the BCM team to reduce network congestion by staggering working hours of staff and requiring the use of audioconferencing instead of network-intensive videoconferences. Where employees are using mobile data to connect remotely, seek service provider agreement to mitigate or waive any thresholds for throttling data throughput during the business disruption. To reduce network impact, ask managed network service providers to identify low-priority traffic or high-bandwidth jobs that can be reduced or rescheduled. Where employees from many organizations are working from home, it is possible that consumer networks will be unable to cope due to widespread use by families in quarantine at home. SPVM teams should work with business units and BCM teams to ensure that alternative systems will be available as needed to supplement bandwidth (for example, portable satellite terminals or fixed wireless WAN in some locations).

- **Availability of Equipment** — SPVM teams must work with providers to rapidly build up stocks of prebuilt laptops in key locations for collection or delivery to employees. Where loaner devices are used, consideration must be given to disinfecting each device as it is returned. Given the potentially high demand for work-from-home infrastructure and the impact of the coronavirus on the global supply chain, there is a high risk of the unavailability of spare equipment through normal procurement channels. SPVM teams should consider sourcing equipment from used (or "second-user") dealers or IT asset distribution (ITAD) service providers (see "Market Guide for IT Asset Disposition"). Peripherals such as keyboards, mice, monitors, webcams and headsets may also be required if employees work from home for longer periods. SPVM teams should work with the BCM and finance teams to decide whether employees can temporarily buy such equipment themselves. If not, agree upon a process for field services teams to supply this equipment when essential.

- **Consideration of BYOD and/or DaaS** — If there are insufficient devices available, SPVM teams must work with business and IT teams to prioritize and allocate devices. Use providers to rapidly

enable bring-your-own-device (BYOD) capabilities, potentially accessing existing virtual desktop infrastructure (VDI) solutions, with an increase in infrastructure to support higher demand. If VDI is not available or not viable, rapid remote working might be enabled by cloud-based desktop as a service (DaaS) solutions. Amazon Web Services (AWS), Microsoft Azure, Citrix and VMware may all be able to rapidly create environments with standard Windows images, or with the organization's own image.

- **Increased Licensing or Subscriptions** — Additional remote working will require additional licenses for key services. In particular, previous business disruptions have shown that remote workers were hampered by a lack of licenses for SSL VPNs, so providers need to advise on whether further licenses should be bought or alternative cloud capabilities should be used. Remote collaboration tools such as Webex or Microsoft Teams may also need additional licenses or SaaS subscriptions, though some providers are also offering free versions of their solution during the coronavirus outbreak (see Note 2). In all cases, though, SPVM teams need to make sure their organization is able to ramp down again following the business disruption, without a longer-term commitment to subscriptions or licenses, perhaps by trading these for a relaxation in SLAs.

- **Use of Alternative Collaboration Tools** — Multiple client demands on existing providers may prevent them scaling for each organization's needs, and some outages have already been reported in collaboration tools, [6] which may require new tools to be found. In this case, other corporate remote working solutions are noted in Gartner's "Magic Quadrant for Meeting Solutions." If these are not possible, SPVM teams should get providers to provide access to consumer collaboration tools such as Slack, Zoom, WeChat or others, but be aware these may experience resource constraints due to extra demand. [7] Ensure clear communication to employees on what type of business information should, and should not, be shared through such services.

- **IT Security Changes** — Providers will need to advise on any security changes necessary to support increased employee remote working. Where employees are working from public network connections and using personal devices, providers should be asked to begin working to deploy endpoint security management onto user devices to ensure secure access to applications and data. Appropriate restrictions on new DaaS environments should be implemented to prevent data from being copied and pasted onto the user device. Examine whether any security policies can be relaxed, such as using guest accounts for employees or using separate network entry points. If a remote-working policy is not in place, use Gartner's "Toolkit: Remote Work Policies" to create one, or ask service providers to provide a copy of a standard remote working policy for employees. Make employees aware of any data security or privacy issues that may apply when working remotely (for example, if GDPR requirements apply to data) and provide them with copies of related policies. For longer-term security, consider the recommendations in "4 Steps to Implement a Perimeterless Digital Workplace."

- **Service Testing** — Work with service providers to test any changes to remote working solutions against a set of basic functional requirements in the time available. Adopt an agile methodology to make quick releases and make corrections as you go. If time allows, arrange with providers to test the solutions ahead of any BC need by sending employees from various locations and business units home to trial capabilities and report issues. Ideally, use employees who have little or no experience of remote working in these trials. Log and take action on any issues as required.

- **Availability of Support** — Any remote working capability will require support, and this may need to be prioritized if employees are sent to work remotely at short notice. Work with the service desk provider to create short guides for remote working: getting started, FAQs and troubleshooting. Set up a service desk process to prioritize any "How do I …?" contacts about remote working issues. Ensure that additional staff have access to the support tools required to assist remote workers, and that there are sufficient licenses for these. If too few provider staff are available, explore whether other in-house IT employees can provide temporary supplemental support.

Any remote working solution needs to include key personnel within service providers' staff, as well as within the organization itself. For example, it may be essential to ensure that those provider staff in the end-user service function who enable security access for remote workers can continue working. In many cases, organizations may only allow such work to be done from the provider's offices, but this will cause an issue if staff cannot get into work (due to illness or government-imposed travel restrictions, for example). Moreover, many staff that provide call center and shared services may not have the equipment available to perform their work remotely. In these cases, SPVM teams should work with providers to supply suitable endpoint and mobile connectivity devices to support such key staff in working remotely, being prepared to pay for extra devices if necessary.

Providers May Struggle to Deliver Services

As the impacts of the pandemic widen, providers of all scales may find difficulty in getting sufficient staff into work to keep service provisions at contracted levels, so SPVM teams must plan for mitigations. If time allows, use the structured approach to BC planning in Action 3, but if more immediate responses are now necessary, then review the suggestions under Action 4.

Action 3: Work With Providers on Contingency Plans

Every service provider should have a business continuity plan, but this may be insufficient to deal with a global issue such as a pandemic. Unlike a flood, typhoon or earthquake, staff cannot simply move quickly to another location — wherever they go, the problem will be there. Working from home sounds like a solution in many places, but as noted above, services may suffer from performance issues when many people use them at once, and it may not even be a viable solution in many emerging economies. When working with the providers of priority services identified by the

business or resulting from the analysis in Figure 2, a structured approach is required to mitigate risks. Figure 3 illustrates the five steps required.

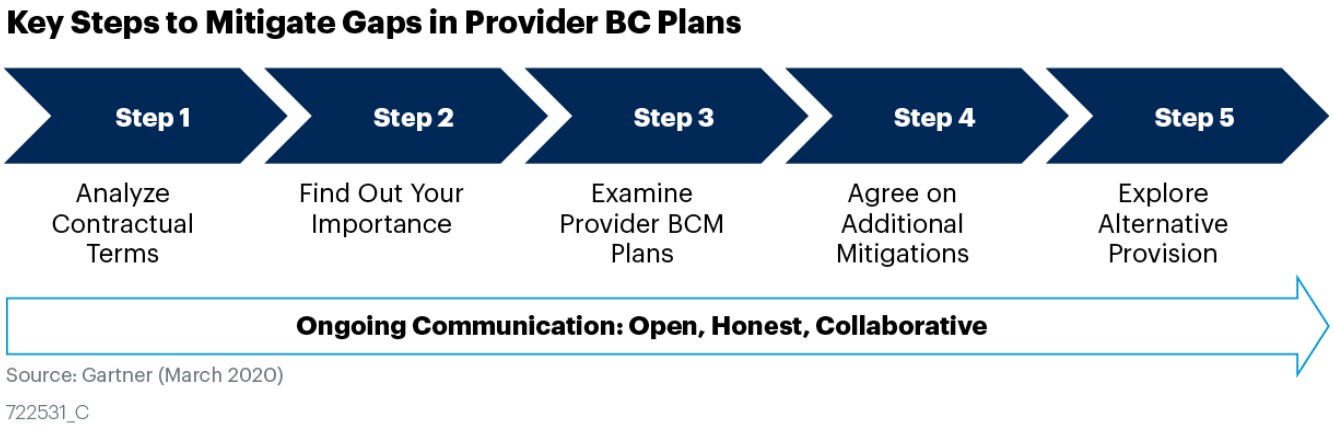

Figure 3. Key Steps to Mitigate Gaps in Provider Business Continuity Plans

The required steps are as follows:

1. **Analyze Contractual Terms** — SPVM teams must start any service mitigation activities by understanding what is in the governing contract. In particular, identify the requirements placed on the provider around BC plans, and how these responsibilities change in the event of a crisis affecting many of its clients at once. While the immediate priority must be to collaborate with providers to implement the BC plan and reduce impacts, if a force majeure situation remains unresolved for a long period, contract termination may need to be an option. Since contract clauses can vary widely, review both the force majeure and termination for convenience clauses, in case termination becomes unavoidable. Determine whether any aspect of the force majeure wording allows the provider to suspend its contractual obligations due to a pandemic, and whether there is a definition of the percentage of unavailable staff required to trigger this situation. See if your organization will be required to carry on paying the provider during such a force majeure situation, and whether it can utilize step-in rights for the service, if essential. If the contract allows for cancellation in the event of force majeure, review the exit plan to see if it exists and how robust it is. Recognize that a provider will struggle to deliver on any exit plan during a business disruption, and that both exiting a contract or utilizing step-in rights are likely to be lengthy and costly.

2. **Find Out Your Importance** — Multiple clients may be calling on your service provider for business disruption risk mitigations or additional services. In this situation, the provider will have to prioritize its key clients' needs and may have preferred-customer clauses requiring this. Alternatively, governments may direct that priority services are given to critical national infrastructure (such as healthcare or utilities). In these cases, SPVM teams must know where their organization sits in the provider's priority list. This will require an open and honest conversation with the provider's account team, but will be essential in determining risk mitigation options.

3. **Examine Provider and Client BC Plans —** Regardless of whether a provider sees the COVID-19 pandemic as a force majeure situation, it should still have BC plans and these should be reviewed in detail. Ideally, this review should be done with the provider, but if the provider is unable to do so, then SPVM teams need to review the BC plans on their own. Identify gaps in the plans and specific impacts that may arise if the provider prioritizes other client work over that of your organization. Provider BC plans are typically based around a catastrophic event at a single location or the reduction in compute or storage capacity caused by loss of a data center, or may assume use of shared BC environments. Such BC plans may not be appropriate in the event of a pandemic, where offices and data centers remain usable, but staff are unable to work from them, or where demand on shared BC facilities is universal. At the same time, SPVM teams must discuss with providers whether their own organization's ability to pay invoices may be compromised by business disruption, and seek agreement to relax penalties for this.

4. **Agree on Additional Mitigations —** Where there are gaps in the provider's BC plans, or where the needs of other clients may impact your organization, SPVM teams must work with providers to agree on additional short-term mitigation actions for services. These will be actions designed to help the provider deliver a skeleton service to an acceptable level by reducing the demand for lower-priority services. Examples of possible mitigations include:

   - **Spreading service delivery across multiple locations.** Where remote infrastructure management services are being delivered from, say, Manila, Cape Town and Mexico City, they will be more resilient to local issues.
   - **Pooling resources.** Where services are currently being delivered by dedicated teams, allowing temporary use of shared resources may ease staffing issues.
   - **Allowing shift work.** Where tasks can be done at alternative times, allowing the provider more flexibility over scheduling will help resource constraints, but may cost more.
   - **Allowing tasks to be done remotely.** Identifying tasks whose security level allows them to be delivered from home or remote locations can allow time used for travel to be converted to working time. SPVM teams should rapidly agree upon any necessary contract waivers to allow this — and some IT firms are already requesting this. [8]
   - **Reducing noncritical SLAs.** Relaxing the resolution times for lower-priority incidents (and the related service credits) and helping the provider to prioritize may allow the provider to still resolve critical incidents within the SLA.
   - **Suspending projects.** Temporarily stopping projects could release staff for other tasks, and reduce change in the environment at a critical time.
   - **Reverting to manual processes.** Where corporate systems fail, it may be possible to use spreadsheets of manual processes to issue bills, for example. In this case, allow the provider time to revert the manual data to the digital form after the business disruption.

- **Increasing automation.** If it is viable to rapidly and safely automate key processes, they will become less vulnerable to staff absence.

- **Utilizing temporary insourcing.** Where suitable employees are available in the organization, certain services may be brought back in-house for short periods of time to protect services, possibly by using managers to provide contingency support for key activities.

5. **Explore Alternative Provision —** Where existing providers cannot provide adequate risk mitigation, SPVM teams will need to explore whether it is viable to deliver services in other ways. Given increased demand by buyers, it may not be viable to utilize alternative providers. However, there will also be providers looking to win more business as a result of the situation, and this may create opportunities to supplement commoditized services. For any new services, examine the time to set up new services, the length of contractual commitment required and the ability to exit the service again after the business disruption has finished. In theory, subscription services such as infrastructure as a service (IaaS) — and, to a lesser extent, SaaS — can be set up very quickly, but may require long-term contractual commitments. With high demand, though, providers will be able to be selective about new clients. SPVM teams must make it easy for such providers to enter new contracts, while protecting their organization, to avoid having providers walk away.

Throughout this time of shared risk, SPVM teams must not fall into the trap of being confrontational with a provider. With providers having multiple clients demanding their attention, they will need to prioritize, and a collaborative approach by SPVM is much more likely to result in a provider being supportive of your organization. SPVM leaders should suspend any benchmarking activities until the pandemic issues are resolved and consider exercising extension options to any contracts coming up for renegotiation. Discuss with providers whether your organization may be better able to support provider staff who are currently onshore, in place of the provider itself.

Regular, open and honest communication between both sides will be essential to the risk mitigation plan, and the response to the pandemic must be treated as a shared problem to solve. To enable this, it will be important to establish contingency communication channels for all services, in case of issues with primary channels. In addition, in order to keep risk assessments (such as that in Figure 2) up to date, SPVM teams should explore with providers whether they can use automated surveys to monitor staff health (see Note 3). If possible, ask providers to report absence rates daily, by country and by site, but do not do this at the expense of compromising providers' work capacity. Consider holding short daily "stand-up" calls with key providers to track developments. It is critical to understand that that provider relationship will last past any crisis.

Action 4: Develop Contingency Plans for Critical Services

If contingency plans become unattainable, providers could invoke force majeure clauses. In the event of a force majeure event due to pandemic, what can an organization do to mitigate the effect on strategic services, especially those in the most impacted countries?

First, SPVM teams should make providers aware that force majeure cannot just be claimed or certified by the national government. Instead, the provider must offer evidence that any pandemic event falls within the force majeure provisions of the service agreement, and that the event materially impairs its ability to deliver services. This is likely to be difficult to prove and would require evidence (see Note 4), and in practice, force majeure claims may fail. However, this will not resolve short-term impacts to the organization if a provider is unable to deliver, and SPVM teams also need to consider specific mitigations that can be applied to individual services. Table 1 provides examples of possible mitigations that could be applied to each service, though it is not intended to be exhaustive.

Table 1: Potential Service Mitigations for the Impact of a Global Pandemic

Service ↓	*Possible Mitigations* ↓
IaaS and PaaS	■ Establish multicloud presence, instead of a single provider. ■ Utilize multiple cloud regions, instead of a single one. ■ Enable brokering of critical services between clouds. ■ Work with providers to move services to highest capacity regions. ■ Reserve instances for critical workloads.
SaaS	■ Migrate “pseudo-SaaS” to Tier 1 IaaS. ■ Mitigate with “burst” or flexible pricing on a consumption basis (see “Consumption-Based Pricing Is Emerging From Leading SaaS Providers, but Beware”). ■ Determine whether unused modules in on-premises solutions provide an alternative.
BPO and BPaaS	■ Move staff onto critical tasks and suspend noncritical services. ■ Explore using crowdsourced or gig workers. ■ Consider temporary insourcing of key work. ■ Ask providers if back-office functions can be shared with those of other clients.

Service	Possible Mitigations
Hosting and Data Center Outsourcing (DCO)	■ Move staff to focus on critical services. ■ Suspend noncritical services (for example, e-learning systems). ■ Reduce backup frequency for noncritical services. ■ Provide laptops to key staff such as system administrators. ■ Allow key staff (or all staff) to work remotely. ■ Consider using retained staff to manage critical operations..
Network Services	■ Increase network bandwidth via bursting or purchased capacity. ■ Support the use of wireless WAN or satellite connectivity as contingency. ■ Explore upgrading existing backup network connectivity to a primary connection. ■ Reduce bandwidth consumption, by stopping low-priority traffic. ■ Reschedule or postpone high-bandwidth usage. For example, reduce video and use audio conferencing instead. ■ Ensure network service providers have stock inventory of replacement equipment.
Service Desk	■ Spread service across multiple delivery centers. ■ Match shift patterns to new working patterns. ■ Direct employees toward self-service solutions. ■ Implement chat-based contact channels and chatbots. ■ Relax SLAs for P3 and P4 incidents. ■ Expedite remote working requests. ■ Consider temporary insourcing of key work.

Service	Possible Mitigations
End-User Support	■ Implement DaaS-based desktops. ■ Allow use of BYOD for remote access. ■ Explore consumer collaboration tools — Zoom, Slack, WeChat, etc. ■ Expand VPN and Webex licensing. ■ Provide laptops to key staff, such as identity and access management (IAM) administrators. ■ Allow key staff work remotely. ■ Stockpile laptops and peripherals in key locations. ■ Consider temporary insourcing of key work.
Application Management	■ Suspend any noncritical application changes. ■ Relax SLAs for P3 and P4 incidents. ■ Spread service across multiple application management centers. ■ Consider temporary insourcing of key work. ■ Ask the provider to introduce a temporary “as a service” offering, sharing staff across clients to support critical applications.
Application Development or Application Implementation	■ Suspend any noncritical projects. ■ Explore implementing “distributed agile” teams across multiple sites (see “Managing Distributed Agile With Outsourced Service Providers”). ■ Explore using crowdsourced or gig workers. ■ Consider temporary insourcing of key work. ■ Evaluate alternative providers, if time allows.
Security Services	■ Spread service across multiple delivery centers. ■ Temporarily insource critical security functions. ■ Implement crowdsourced security services.

Gartner (March 2020)

SPVM leaders should not apply the mitigations in Table 1 in a blanket fashion at the start of the crisis. Instead, the decision on which mitigations to apply (if any) should be governed by the needs of each organization's BCM plan, by the guidance given by the BCM team and by the service prioritization noted earlier. Where SPVM teams apply multiple mitigations without appropriate governance, any crisis situation may well be worsened due to the sudden service changes that would be introduced during a time of least organizational resilience.

The Pandemic May Impact the Economic Outlook

While the long-term impact of a coronavirus pandemic is unknown, it is highly likely that it will negatively impact the global economy and individual organizations' revenue, and this possibility has already caused central banks to cut interest rates. [10] As organizations start to recover from the operational impacts of the virus, they are likely to have to address these issues. For SPVM teams in many organizations, this will mean a requirement to optimize the costs of services, using Action 5 below.

Action 5: Plan for Longer-Term Cost Reductions

As the longer-term impacts of the pandemic become obvious in the global economy, SPVM leaders are likely to need to consider additional strategies for reducing ongoing costs in services. Consider approaches such as optimizing the labor used, reducing demand, amending SLAs, increasing service automation, looking at global delivery locations (onshore, nearshore, offshore), negotiating more flexible mobile data service consumption options and rationalizing service portfolios. A wide range of further possible options can be found in Gartner's research in this area. For example, see "Take Steps to Improve Productivity and Optimize Outsourced Infrastructure Services Costs" and "Cost Optimization and Productivity Strategies in Application Services for Short- and Long-Term Returns."

In the short term, SPVM leaders must ensure that in addressing current coronavirus risks, they try as far as possible to avoid any longer-term cost commitments. This will involve considering questions such as:

- Will a short-term usage of SaaS solutions result in higher ongoing costs as providers charge according to peak usage?
- Will a shift in geographic usage of regionally licensed SaaS or software solutions require additional subscriptions or licenses?
- Can additional licenses or subscriptions be terminated after short-term use, with no ongoing charge?
- When does the period of free use of a collaboration tool expire and create a cost for the organization?
- Will an increased proportion of "How do I …?" calls to the service desk increase charges?

- Can increased network bandwidth be paid for by bursting, rather than increasing fixed-capacity commitments?
- Will additional temporary use of mobile data trigger high overage costs or slowing of data speeds under service provider traffic management clauses?
- Does reduced business activity during the period of business disruption mean that fixed prices or collars on pricing need to be negotiated away?

Acronym Key and Glossary Terms

BC	business continuity
BCM	business continuity management

Evidence

1. See the WHO's declaration at WHO Director-General's opening remarks at the media briefing on COVID-19 — 11 March 2020.
2. See the report in the Financial Times, "China Issues Record Number of Force Majeure Certificates," from 28 February 2020.
3. See, for example, the Guardian story "From Confidence to Quarantine: How Coronavirus Swept Italy," from 10 March 2020.
4. See, for example, the tracking available at Johns Hopkins University or at Worldometer.
5. For example, Facebook, Google, Twitter and Amazon have implemented remote working for employees, as noted in the CNN News article, "Big Tech Firms Ramp Up Remote Working Orders to Prevent Coronavirus Spread" from 12 March 2020.
6. See, for example, "Microsoft, Google, Slack, Zoom et al Struggling to Deal With a Spike in Remote Tools Thanks to Coronavirus."
7. For example, see reports of a European outage of Microsoft Teams at "Microsoft Teams Outage Affecting Users in Europe."
8. For example, see the predictions by Bloomberg, at "Coronavirus Could Cost the Global Economy $2.7 Trillion. Here's How."
9. The interest rate cut by the U.S. Federal Reserve is reported by CNBC at "Federal Reserve Cuts Rates to Zero and Launches Massive $700 Billion Quantitative Easing Program." The interest

rate cut by the U.K.'s Bank of England is reported in this BCC article: "U.K. Interest Rates Cut in Emergency Move."

0. For example, see the discussion of the issuance of force majeure certificates by the Chinese government at "Coronavirus Outbreak: Global Guide to Force Majeure and International Commercial Contracts."

1. More details on the legal principles behind force majeure can be found at, for example, Trans-Lex.

2. India's Economic Times reported on providers' request to waive restrictions on work locations in "Covid-19 impact: IT Firms Seek Client Waivers So Staff Can Work From Home."

Note 1: Force Majeure

A force majeure clause (French for "superior force") is a contract provision that relieves either party from performing its contractual obligations when certain circumstances beyond its control arise. In this case, the words "pandemic" or "epidemic" in the force majeure clause of a contract may excuse one party from its obligation. There is also the possibility of "acts of God" and "acts of government" (for example, in imposing travel restrictions) being used in the case of the coronavirus. Note that many providers' contracts include a restriction that says that a force majeure event does not excuse the client's payment responsibilities. In addition, the fact that a contract becomes economically burdensome or less advantageous for a party does not qualify as a force majeure even if a loss in revenue may have been caused by the event. Nor does a change in market conditions affecting the profitability of the contract constitute a force majeure event. [11]

Force majeure rights can also vary greatly by legal jurisdiction and by how they are written in the contract. Some jurisdictions will take an implied view of force majeure, and others require that it be directly stated in the contract. Until appropriate declarations are made by national governments, courts may not uphold force majeure (see Note 3), so it is important to understand the rules of each jurisdiction and how force majeure is defined in each specific contract. For one example of a discussion of the legal issues, see "Coronavirus: Force Majeure for Chinese Contractors Overseas" (Pinsent Masons).

Note 2: Free Offers From Providers

In light of the COVID-19 pandemic, a number of providers are making their solutions available for free temporarily. For example:

- Microsoft Teams, Google Hangouts, Cisco Webex, Zoom and LogMeIn are all reported as offering free temporary versions in certain circumstances — see "Free Video Conferencing: Coronavirus Spurs Special Deals From Webex, Google, Others" (ZDnet).

- SAP has opened up its Ariba Discovery solution to allow clients and providers to easily find each other during the period of disruption.

- Salesforce is allowing some free access to its offerings.
- Lakeside analytics is offering free access to its remote work planning solution.

Note 3: Automated Monitoring of Impacts

Some providers of robotic process automation (RPA) solutions and other tools are providing solutions that allow regular automated surveys of staff health to be conducted. These surveys create a daily report on staff status and can streamline reporting. See, for example, the tool from UIPath at "Health Screening Bot." It may also be possible to integrate data on the spread of the virus with analytics data on the physical location of endpoint devices to identify the levels of risk in each location in real time.

Note 4: Evidence for Force Majeure Claims

To claim a force majeure situation, a provider must be able to offer evidence that the event was outside its control and that it impaired its ability to deliver. The contract may specify the required evidence, though many contracts do not. However, at a minimum, a provider should be able to show that the government of the affected country made a declaration at national level, such as declaring a national disaster or making a disease notifiable. In addition, that declaration may only be valid within the specific country itself, and not be valid for cross-border contracts. [12] As the required evidence will vary by country, SPVM leaders must get legal advice on what evidence is suitable for each location. Also, if the provider did not have adequate BC plans, or did not exercise them appropriately, it may still be possible to make a claim for business interruption. SPVM leaders need to work with legal teams to decide whether they wish to do this, even in the event of force majeure being accepted.

This complimentary research is part of Gartner's ongoing coverage of the business impact of the coronavirus (COVID-19).

Access additional free content and coverage at gartner.com/smarterwithgartner and gartner.com.

Become a Client

Get access to this level of insight all year long — plus contextualized support for your strategic priorities — by becoming a client.

gartner.com/en/become-a-client

U.S.: 1 800 213 4848

International: +44 (0) 3331 306 809

About Gartner

Gartner, Inc. (NYSE: IT) is the world's leading research and advisory company and a member of the S&P 500. We equip business leaders with indispensable insights, advice and tools to achieve their mission-critical priorities today and build the successful organizations of tomorrow.

Our unmatched combination of expert-led, practitioner-sourced and data-driven research steers clients toward the right decisions on the issues that matter most. We are a trusted advisor and an objective resource for more than 15,000 enterprises in more than 100 countries — across all major functions, in every industry and enterprise size.

To learn more about how we help decision makers fuel the future of business, visit gartner.com.

Gartner