



COVID-19, Vendor Management & Managing the New Normal



COVID-19, VENDOR MANAGEMENT & MANAGING THE NEW NORMAL

Executive Summary: How are financial institutions' critical vendors holding up as the COVID-19 pandemic spreads? That's a vendor management question every FI should be asking. This whitepaper helps financial institutions consider how their approach to vendor and business continuity management align with regulatory guidance while offering insights into key elements of a critical vendor's pandemic plan; what to do when a vendor can't perform; and predictions of what the new normal will look like.



How are financial institutions' critical vendors holding up as the COVID-19 pandemic spreads?

That's a vendor management question every FI should be asking.
It's not just a best practice. It's a regulatory requirement.

The FFIEC Pandemic Planning Guidance reminds FIs that business continuity management (BCM) should address the threat of a pandemic outbreak to critical services. It's all about assessing the risk that a pandemic-related disruption will prevent a critical vendor from performing.

While regulators recognize that it's a busy time for financial institutions, there will also come a time when the COVID-19 threat has passed and examiners will want to assess how FIs performed, including in vendor management. That makes it important to maintain documentation for vendor management and BCM during the pandemic.

The vendor management lifecycle for BCM breaks down into four parts:

- 1. Risk assessment.** Is this vendor critical to everyday operations?
- 2. Due diligence.** Does the vendor have a business continuity plan (BCP)?
- 3. Contract structuring and review.** Does the vendor contract define BCM expectations, include monitoring tools like test results, and address remedies?
- 4. Ongoing monitoring.** Is the plan in force, updated, and tested at least annually?


The vendor management lifecycle is critical for managing *critical vendors*, or vendors that provide critical functions, infrastructure, or processes on a regular basis. Critical vendors require much more oversight than other third-party vendors, so the label should only be given to vendors with high inherent risk (i.e. there would be a serious and substantial problem if the vendor failed to perform).

Assessing Critical Vendor Pandemic Plans

In an ideal world, a critical vendor would have a BCP and provide tests of that plan, including pandemic results. Unfortunately, the vast majority of BCP tests conducted before COVID-19 don't test pandemic plans.

The good news is that vendor BCPs are likely to include and test mitigation strategies that have been implemented as part of its pandemic response. For example, it might include plans for working from home and a test of the plan, including insights into how well security worked. Looking at these tests and results can provide some assurance of critical vendor preparedness.

FIs are also interested in how critical vendors are responding to the pandemic in real-time, including where they get their information and how plans are evolving to keep pace with changing circumstances. The problem, though, is



that both FIs and vendors are currently inundated with a variety of new challenges and may have limited time to discuss details of vendors' pandemic response.

If there isn't time to fully reassess how vendors are operating from a control standpoint, FIs should document the outcome instead, focusing less on process and more on results. For instance, there is no way of verifying that a vendor is following social distancing protocol, but as long as the vendor is able to continue to provide services, it should serve as enough assurance.

Before inundating a vendor with questions, FIs should understand what areas are the most important to ask about and concentrate their questions there. Otherwise, you'll overwhelm vendors with questions and then potentially overwhelm the FI by having to sort through all the responses.

ELEMENTS OF A CRITICAL VENDOR'S PANDEMIC PLAN

When reviewing a critical vendor's pandemic plan, here are some of the key areas to consider:

Finances

Addressing COVID-19 is expensive and can cause financial distress, especially for startups and other young companies. Great pandemic planning won't save a company if it doesn't have the funds to support it. Revisit your vendors' finances to assess if they are well capitalized or if their continued viability is contingent on growth that has suddenly slowed.

Information about a critical vendor's financials should be guaranteed in your vendor contract. Documents like SSAE 18s, SOC-1s, insurance certificates, and publicly available data should be monitored regularly since a major change in any of these documents is cause for investigation. The earlier your FI suspects a vendor is having financial difficulties and may stop providing services, the more time it'll have to find an appropriate replacement.

Identifying a troubled vendor can be hard, especially if financial information comes just once a year. SSAE 18s are a good indication that a company is in a strong financial position. SSAE 18s are expensive and a sign the audited company is financially healthy. Conversely, changing auditors may be a sign of trouble since operations could be trying to cut costs. It also might be nothing. Make sure you dig into the details so you don't overreact.

One caveat: Don't analyze vendors like a loan applicant.

Just because your institution wouldn't lend to a vendor doesn't mean it's not financially sound. Sterling A credit is not a necessity. For example, large companies leverage up to buy other companies.

On paper it might look like they are unhealthy, but these service providers are preparing for the future—investing in companies that will help them keep pace with evolving technologies and maintain their competitive position.



Personnel

If a vendor experiences a COVID-19 outbreak across its staff, it can hinder its ability to deliver products and services. The challenge is there's a lot of recommendations and controls for limiting the transmission of COVID-19 among personnel (following recommendations and best practices), but no way to test it. Instead look at the consequences instead of the controls. If staff is available and still getting the job done, assume those controls are working.

It's much easier to get information on IT controls (thing like firewalls, access control, GLBA/privacy, and work product quality) for employees working at home. A SOC-2 report is the best source of information since everything is verified by an independent auditor.

Geography

Many core processing vendors weren't initially in hot spots, but what may occur when it gets there?

IT & Data Center Recovery

A whole company may not have to close, but it may have to shutter a site in the event a geographic area experiences a high infection rate. Does the vendor have backup sites, especially data centers, that are geographically dispersed?

If vendors use third-party hot sites will the vendor have the capacity to support operations in the event of a regional or large-scale event? Will it have the same security controls? What are the recovery time objectives?

Keeping Up with Demand

With more financial institutions using digital channels, does the vendor have the capacity to keep pace?

Fourth-Party Risk

Are vendors' critical third-party vendors prepared? That should be well documented in audits.

Supply Chain

Can the vendor provide or replace critical components/hardware when needed? Does the vendor have a backup?

Implementation Delays

Whether it's a core conversion or other smaller undertaking, will staffing or other COVID-19-related issues delay new product implementation? The answers can impact everything from financial projections and marketing initiatives to strategic goals.

Communication

Have clear communication contacts both on the vendor and FI side. A business impact analysis should already make it clear who within the FI is responsible for communicating with vendors and ensuring the vendor provides important updates.



KEY QUESTIONS TO ASK VENDORS

It's important to understand the contingency plan of vendors as you work with them during the pandemic. Your FI should have already reviewed critical vendors' BCPs as part of its own ongoing vendor and business continuity management programs. Questions to answer include:

- **When was the last time you updated and tested your BCP and do you have a pandemic plan?**
- **What are you doing to monitor the situation?**
- **How will you communicate ongoing updates to us?**
- **How will you continue to provide services in event of large-scale employee absenteeism?**
- **What if you are unable to use one or more offices or sites?**
- **Will this delay the delivery of support, new products, services or updates?**
- **Are your (vendor's) critical third-party vendors prepared?**
- **Are you financially prepared to weather coronavirus?**
- **Has your company assessed the risks of COVID-19 to your business? If so, please describe the results of your risk assessment.**

Many of these questions can be answered by reviewing a critical vendors' BCP. Other questions may require reaching out to vendors. Many vendors are doing a phenomenal job with their response to COVID-19 and are happy to share documentation demonstrating that working with them is low risk.

WHAT TO DO WHEN A VENDOR CAN'T PERFORM

In the event a vendor can't perform, it might try to enact a force majeure clause, a clause in the contract that creates an exception to a performance. There's no universal definition of a force majeure. It may include a reference to "Acts of God," which typically encompasses natural disasters (tornadoes, floods, blizzards). It may include pandemics, epidemics, or disease, triggered based on a declaration by a recognized body like the CDC.

FIs should have counsel review the specifics of the agreement to determine whether COVID-19 triggers this provision. If a vendor contract has an applicable force majeure provision, your FI needs to figure out what, if any, relief it gives the vendor and whether the FI will still have to pay for services. For example, if a vendor is supposed to come on site for maintenance but can't travel due to COVID-19, how will that be handled?

If the vendor relationship can't be saved, an FI should review its vendor contract to understand how it will impact the FI, especially in terms of costs like termination fees. Your FI's BCP should



have plans for responding to a vendor outage, regardless of the reason it's caused.

CRITICAL VENDORS VS. VENDORS CRITICAL TO BCP

When developing BCPs, remember there is a difference between critical vendors and vendors critical to BCP. Existing critical vendors are essential to your everyday operations. Recovery plan providers are alternate third-party vendors like generator providers, alternate sites, and backup service providers. These vendors might be critical to your BCP, but not on a day-to-day basis. As a result, they don't require the intensive due diligence work of a true critical vendor. To help differentiate the two, it's useful to use different terminology (critical vendor vs. recovery plan provider) to avoid creating unnecessary work.

Recovery plan providers play a key role in any BCP. FIs should ensure they have identified and potentially prearranged a comprehensive set of alternative resources. They should assess these vendors' immediate or short-term space, systems, and personnel to determine if it has the capacity to absorb, assume, or transfer failed operations. FIs should outline disruptions that may require the use of alternate TSPs.

Recovery plan alternatives may take several forms and involve the use of other data centers or third-party service providers. FIs should identify the most plausible range of recovery options and develop business continuity plans that address restoration of key services.

Any recovery arrangements with a third-party vendor should require a legal contract or

agreement. Operations critical to functioning should establish prompt recovery objectives, such as same-day business resumption and consider things like increased risk of failed transactions, liquidity concerns, solvency, and reputation risks. The FI must also describe its reasons for choosing a particular alternative and why it is adequate based on the FI's size and complexity. Areas to cover should include:

- **Core operations**
- **Data processing**
- **Facilities**
- **Infrastructure systems**
- **Suppliers**
- **Utilities**
- **Interdependent business partners**
- **Key personnel**
- **EFTs**
- **Cash providers, delivery services & transportation providers**

THE NEW NORMAL: WHAT TO EXPECT

Eventually the U.S. will be able to lift shelter-in-place orders and the crisis will become less acute. When that happens (whether its Q3, Q4, or some other time), a new normal will emerge.

As with past crises and their ongoing influence, the pandemic will have a huge impact on how we do business going forward. Likely predictions include:

- **BCM and BCPs will be broader in scope.**
- **COVID-19/pandemics will be addressed in future vendor agreements.**
- **Regulators will be looking closely at both internal and vendor BCM.**



BCM & BCPs Broader in Scope

Before COVID-19, BCPs were mostly focused internally on the financial institution itself. It addressed how to respond when the business climate was affected by a disaster, how to correct how issues within the business model, and how to get systems back up.

It also assumed the problem would be a local or regional issue, not a worldwide pandemic. BCPs will not longer be limited to “What do we do when we can’t access our office?” They won’t be as simple as “we’ll work from home.” It will be far bigger than that. BCPs will need to plan for the cascading effects of a mass event. FIs will need to think bigger and more broadly about business assumptions and impact. For example, FIs might ask questions like:

- **How can we support consumers/members if the business world changes?**
- **What if a key client segment faces economic hardship?**

VENDOR AGREEMENTS

Contracts are a control to help manage vendors and help ensure your financial institution maintains operational continuity. As we focus more broadly on BCM, well-written vendor contracts will include BCP provisions that:

- **Define key business continuity terms;**
- **Require evidence of ongoing business continuity planning; and**
- **Detail performance standards.**

BCP addendums for existing contracts are likely to become very popular and far more favorable to FIs. This includes evidence of BCP testing, performance standards, and termination provisions for BCP failures. Addendums and new agreements will help FIs retain leverage when it comes to pandemic planning and disaster recovery to ensure they can get all the details and answers they need to test vendors plan as an element of their own plans.

This information can help an FI decide how necessary it is to supplement a contract’s exit strategy and termination clauses by researching and having access to alternate service providers.

When preparing contingency plans, FIs should leverage contracts to:

- **Ensure that a disaster recovery and BCP exists for contracted services and products.**
- **Assess the adequacy and effectiveness of a service provider’s disaster recovery and BCP and its alignment to the FI’s own plan .**
- **Document the roles and responsibilities for maintaining and testing the service provider’s business continuity and contingency plans.**
- **Test the service provider’s business continuity and contingency plans on a periodic basis to ensure adequacy and effectiveness.**
- **Maintain an exit strategy.**

REGULATORS & EXAMS

While regulatory agencies can postpone exams when disaster strikes, when exam time finally does come they will have an expanded focus on:

- **Business continuity plans**
- **Response**
- **Post-disaster risk management**

Examiners will be very interested in the effect of COVID-19 on your institution. Make sure your FI has documentation on what's it doing, how it's doing it, and what its BCP and pandemic plans are moving forward. These will all be major points of discussion and may even impact CAMELS or ROCA ratings going forward, as noted by The Interagency Supervisory Examination Guidance for Institutions Affected by a Major Disaster issues in December 2017, which warns that regulators will be very interested in an FI's BCM and BCP after a disaster.

We can also expect new BCM guidance just like we saw increased interest in risk management after the financial crisis in the 2000s. Not every FI or critical vendor will have had effective plans for dealing with COVID-19. Their mistakes will influence new regulation and guidance.

Regulatory priorities may shift. We've already seen several new regulatory initiatives postponed. It's possible it may delay big projects too, such as the NCUA's planned shift to the new MERIT exam. We may also see regulators trying to move to more remote exams so they aren't as reliant on face-to-face meetings.

BEST PRACTICES FOR ALIGNING BCM AND VENDOR MANAGEMENT

As the COVID-19 pandemic continues, the connection between BCM and vendor management is getting more and more attention. Increase awareness of critical vendors' pandemic response and prepare for a future where critical vendor BCM is top of mind for regulators with these best practices for ensuring vendor management and BCM align:

Coordinate policies

Draft your BCP and vendor management policies together using the same definitions and with the same goals in mind. When BCP and vendor management are coordinated at a policy level, it leads to coordination in carrying them out.

Use proper risk assessment methodologies

Vendor management and business continuity should identify critical vendors together. Align the risk a vendor presents with the institution's overall strategy. Each critical vendor creates extra work, so limit the designation to third parties that truly present a substantial risk.

Analyze agreements

The best opportunity to minimize risk is at the start of a contract. Business continuity and vendor management should work together to spell out requirements and expectations before contract negotiations—including audits, documents and timelines for receiving them. It's not enough for your vendor to say that it's compliant—an FI needs the tools to do the due diligence and prove it.



Monitor proactively

Divvy up monitoring responsibilities across business continuity planning and vendor management and share the results. This includes:

- **Annual reviews with expected vendor documents (SSAE 18s, disaster recovery plans and tests, incident response plans and tests, financials, summary findings and evaluations).**
- **Ongoing monitoring (litigation, sale or acquisition of the vendor, data breaches, regulatory issues and financial performance).** Due diligence isn't only for before a contract is signed.


BCM is never done

Just because a vendor has a 100-page BCP doesn't mean an FI can check the box and move on. What's inside matters. Vendors should test BCPs with a CPA firm or licensed professional to make sure its meeting standards at least annually. Circumstances are always changing. BCPs should reflect those circumstances, otherwise critical vendors may not be prepared for pandemic.

Recognize that a pandemic has no pre-defined end. That makes BCM a fluid process. Vendors should have plans for different scenarios: What if it lasts 3 months? 6 months? 9 months? Far-out plans don't have to be detailed, but there should be what-ifs and plans for allocating resources.

While we don't know how long the COVID-19 pandemic will last, FIs need to be prepared for the long haul—and so must their critical vendors. Find the time to review critical vendors' existing BCM and pandemic-related testing and reach

out to them if there are any gaps. Make sure new vendor contracts provide controls for ensuring the vendor is prepared for pandemic and other business disruptions. Oversight of vendors is ongoing and you need to know when a backup plan is likely to be needed.

Your FI shouldn't be caught off guard by a critical vendor that can't perform. 

About Ncontracts

Ncontracts provides risk management and compliance solutions to a rapidly-expanding customer base of more than 1,400 financial institutions located in all 50 states and U.S. territories. The company's powerful combination of software and services enables financial institutions to achieve their risk management and compliance goals with an integrated, user-friendly, cloud-based solution suite that encompasses the complete lifecycle of operational risk.

Visit www.ncontracts.com.