UNCOVERING UNKNOWNS

Understanding the Intersection of Vendor Management and Business Continuity Planning

CONTRACTS
The Upside of Risk

(888) 370-5552
info@ncontracts.com
www.ncontracts.com

EXECUTIVE SUMMARY: Financial institutions aren't just responsible for their own business continuity plans—they must also ensure that critical vendors have properly drafted, executed and tested plans. This requires that institutions recognize the connection between vendor management and business continuity. By uniting the efforts of these two teams, institutions can develop better approaches to risk assessment, due diligence, contracts and monitoring resulting in more efficient operations and a stronger business continuity plan.

Introduction

Disaster can strike at any time. From hurricanes and wild fires to cyberattacks and terrorism, unforeseen events can disrupt a financial institution's operations and cause losses.

It isn't a rare occurrence. Natural catastrophes caused $16.1 billion in insured losses in the U.S. in 2015, and FEMA declared 43 major disasters.

While financial institutions can't predict when and if such events will happen, they must plan for the possibility. Every institution is required to have a business continuity and disaster recovery plan in place to quickly resume key business operations in the event of a disaster—limiting impacts and losses.

But it's not enough for an institution to develop and test its own business continuity plan (BCP). Institutions are required to evaluate and monitor critical vendors to ensure they have strong business continuity plans as well. If an institution is dependent on a third-party vendor that's incapable of surviving a disaster, then its own business continuity plan has failed.

Unfortunately, not every financial institution recognizes this link between BCP and third-party vendors. As a result, the team responsible for business continuity planning often doesn't think to reach out to the vendor management team or consult vendor management guidance when drafting BCP policies. This not only negatively impacts the institution's overall business continuity planning, but it wastes time and resources.

Business Continuity-Vendor Management Overlap

Regulators have been monitoring third party service providers since The Bank Service Company Act of 1961. More recently, the Federal Financial Institutions Examination Council (FFIEC) added vendor risk management to its examination manual in 2004. This is outlined in Appendix J: Strengthening the Resilience of Outsourced Technology Services. Additionally, the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC) and the Federal Reserve have released their own guidance on vendor management.

While each agency uses its own language, all vendor management guidance essentially says the same thing: financial institutions, particularly the board and management, are responsible for identifying and controlling the risks of third-party relationships—including subcontractors. Institutions can outsource activities, but they cannot outsource the risk.

This pertains to every aspect of vendor relationships—including business continuity planning—placing responsibility for third-party resiliency and business continuity planning squarely on the shoulders of financial institutions.

If an institution is dependent on a third-party vendor that's incapable of surviving a disaster, then its own business continuity plan has failed.

While it's a big job, regulatory guidance offers a framework to help institutions identify and mitigate the risks posed by third-party vendors. It includes:

- **Risk assessment**
- **Due diligence in selecting a vendor**
- **Monitoring**
- **Contract structuring**

Properly executed, the elements of the framework can provide the tools and knowledge necessary to ensure vendors have strong BCPs in place. Unfortunately, silos between business continuity planning and vendor management often get in the way. Unaware of the overlapping guidance, each team works independently, creating a series of problems.

First, teams often duplicate work, wasting time and resources as different people read the same agreements. Worse yet, duplication creates inconsistencies as each team maintains separate standards and files. For instance, if business continuity is following its own guidance for maintaining lists of third-party service providers, vendor management may be doing the same, resulting in separate lists or vendor categories—an issue that can catch the eye of regulators.

Second, the teams aren't leveraging each other's strengths. Rather than align policies and procedures, each team drafts its own without the other's input, potentially creating inefficiencies and headaches. Vendor management may unknowingly draft procedures that hinder the BCP team's efforts instead of helping maximize efficiency.

Third is the issue of vendor contracts. Guidance recommends that vendor contracts address the financial institution's BCP testing requirements. If the teams aren't working together to identify and communicate the necessary requirements, important provisions may not make it into the contract.

To avoid these problems and others, business continuity and vendor management need to jointly address the four elements of a strong vendor management framework to ensure the proper controls are in place.

Risk Assessment

What is a critical vendor? The answer depends on who you ask.

Business continuity regularly defines critical vendors—often emphasizing physical infrastructure. Vendor management also defines critical vendors, often considering other risk factors such as financial or reputational risk.

In reality, a critical vendor is any vendor that could cause material harm to the bank. Yet it's not always clear which third-party vendors deserve the label—and the extra work that goes along with it. Guidance on critical vendors is subjective, qualitative and not very specific.

Ultimately it comes down to what the board and directors consider a material risk, and it's different for every bank. An institution's size, complexity, location, risk factors, offerings and other factors all play a role. Just because a policy for defining critical vendors is effective at one institution doesn't mean it will work at another—it may be a case of trying to put a square peg in a round hole.

A variety of factors must be considered when drafting a policy for risk assessing vendors:

Access. Just because a company has access to an institution's data, doesn't mean it's a critical vendor—it's the type of data that matters.

If a vendor is transmitting or storing Gramm-Leach-Bliley protected customer data, it has the potential to materially harm the bank with a data breach. That includes core processors, item processors, ACH and mortgage vendors and anyone else processing transactions. Breaches of these vendors pose a huge reputational risk as clients lose trust in the bank's ability to protect their data—not to mention the regulatory action it can bring. Just think of the aftermath of Target's well-publicized data breach in 2013.

Just because a company has access to an institution's data, doesn't mean it's a critical vendor—it's the type of data that matters.

Yet not all data has the same risk. For instance, employee data should be protected, but if a garbage truck loses a trash bag of W-2 forms it's not going to create a regulatory nightmare. In fact, if you were to treat every vendor with access to employee data as a critical vendor—including the vision company, health insurance vendor, payroll company and expense report vendor—it would create a huge, unnecessary workload.

Frequency. A vendor may have only occasional access to data. For instance, many institutions may use a huge firm for records management and data backup. Bank A may use the firm to store all its protected data on the cloud. Bank B might just use the firm's services to shred documents on site. It's the same firm, but completely different services. One accesses and transmits data regularly. The other has occasional on-site access. Consider how often your institution uses a vendor and in what way.

Dependency. Not every bank is equally dependent on major vendors. For instance, a rural bank in Minnesota may have just one telecom provider in the market, meaning they have only one possible way to access the internet. That may make telecom a critical vendor. Yet a bank in Minneapolis may have many service options and is far less dependent on a single vendor. Ask how much your institution relies on a vendor.

Replaceable. The more married the institution is to the vendor—for instance, core processors or a contract that's cost prohibitive to terminate—the more likely it is to be critical. Consider the ease or difficulty of replacing a vendor.

Client impact. If a vendor fails, will it have a material impact on the client? This may include vendors like credit and debit card processors or insurance services. The greater the likelihood of a vendor failure having a measurable impact on clients, the more likely it is to be a critical vendor.

Financial impact. Determine whether the bank's P&L or balance sheet would be materially impacted by a vendor relationship. For instance, if the bankers bank where an institution sweeps all it funds went under, it would create huge financial loss. If a vendor could cause material financial harm, it should be considered a critical vendor.

Due Diligence

When it comes to due diligence, different guidance use different terminology—risk assessment, due diligence, diligence—but they are all talking about the same thing: a pre-contract risk assessment.

In addition to the typical due diligence necessary for every vendor, financial institutions should also thoroughly examine critical vendors' business continuity plans to understand how they align with the institution's own BCP. It's not enough to ask if it exists. You need proof of its functionality, especially its recovery capabilities. Guidance suggests due diligence include:

Third-party capacity. If a vendor faces disaster, your institution probably won't be the only one affected. That's why it's important to determine if the vendor has the capacity to restore every client within its recovery time objectives and recovery point objectives. In the event it cannot quickly restore services, the vendor should have a workable agreement lined up with an alternate provider—or else the institution must find its own back up vendor as part of its BCP.

Third-party management. Just like financial institutions, many vendors outsource activities to service providers. These subcontractors must also have effective BCPs. The prime vendor should regularly review them and conduct its own due diligence—otherwise your institution will have to do it. Ultimately, regulators view it as the institution's responsibility.

Cyber threats. From malware to distributed denial of service attacks (DDoS) to insider threats, vendors must be able to respond to cyber attacks and have an actionable incident response plan. They also must stay on top of emerging threats. This is particularly important for vendors using the cloud.

Testing. Guidance strongly encourages regular testing of vendor's business continuity plans and examining the results to identify potential problems. Before signing a contract, be sure to ask for results of the vendor's last business continuity test, especially for critical vendors.

Never let a vendor's reputation or size substitute for actual testing. Disasters can happen at any time to even the biggest names. For instance, in 2012 Super Storm Sandy flooded the new item processing center of a major core processor. The flood impacted over 100 of the company's core banking clients, disrupting item processing.

While no one could have predicted Super Storm Sandy, institutions that were very diligent about business continuity planning might have been able to avoid the problem of using the flooded center. An agreement between regulators and the company after the fact revealed "unsafe and unsound practices relating to the TSP's disaster recovery and business continuity planning and processes." Institutions that asked the right questions and then followed their own BCP policies may have held off on moving to the new facility—and avoided a major service interruption.

Monitoring

Testing is just as important—if not more important—after the contract is signed as institutions need to proactively monitor vendors. This includes two elements: the annual review and ongoing monitoring. The annual review includes the documents and results an institution should expect from its vendors: Statement on Standards for Attestation Engagements 16 (SSAE 16s), disaster recovery plans and tests, incident response plans and tests, financials, summary findings and evaluations.

Tests should demonstrate that the vendor (and any subcontractors) and the institution will be able to recover and resume operations within contractually specified parameters. When possible, financial institutions should be active participants in tests, guidance suggests. Results should be carefully reviewed to identify issues and then tracked to ensure any problems are resolved. Critical vendors should be tested annually, if not more often.

Ongoing monitoring goes beyond the annual assessment to keep the institution aware of any major concerns including: litigation, sale or acquisition of the vendor, data breaches, regulatory issues and financial performance. For instance, if a vendor has a publicized data breach a few days before your scheduled database migration to its platform, you'll want to know about it. If you go through with the move despite the breach, you'll want to be able to justify the decision to regulators.

All monitoring should be documented and issues should be brought to the institution's board of directors if necessary. Findings may necessitate revisions to the institution's BCP or changes in the contract with the provider.

Leveraging the Contract

The best way to ensure vendors are complying with an institution's business continuity plan is to spell out requirements and expectations in vendor contracts. But that can only be done when business continuity works in tandem with vendor management to identify requirements. If vendor management doesn't know what to ask, it won't be included in the contract—and once a contract is signed vendors are far less motivated to meet demands.

Guidance suggests institutions address these nine areas to ensure vendor contracts support BCP requirements:

1. **Right to audit.** Make sure you have the right to review the internal operations of the vendor or have access to audit documents. Spell out the level of notice required, what the bank is allowed to see and who performs the audit. Add provisions that require data to be shared to prove cyber security measures are in place.

2. **Monitoring performance standards.** Define how the vendor can be measured, including up time and volumes, and how it will respond to requests. Be wary of any contract that doesn't mention performance or response times. It should specifically detail expectations or service level agreements.

3. **Breaches.** The consequences of a breach should be clearly detailed, including whether the institution can terminate the contract, how long the vendor has to remedy the problem and what, if any, remedies beyond termination are available.

4. Subcontracting. If a contract doesn't specifically prohibit it, then a vendor can transfer its rights and responsibilities to another vendor via outsourcing. If a contract specifies that subcontractors will be used, the institution may need to conduct due diligence on that vendor as well. Make sure all contracts require notice and consent before a vendor outsources.

5. Foreign-based service provider. It makes a difference where your vendor is based, particularly if you're using the cloud for storage. Know which states your vendor is registered in and if they are in good standing. If it's based in a foreign country, it should have an insured U.S. subsidiary. Most important, data should not leave the United States. If your cloud provider plans to send your data to a data center in India, the potential liabilities are huge and you must conduct due diligence on that facility—a far more complicated task.

6. Business continuity plan testing. Your vendors must have a business continuity plan and test that plan. The contract should outline how often they are required to test their plan and how fast they must be back up and running. The more critical the vendor, the more detailed the plan should be.

7. Data governance. Contracts should address data governance including how data is handled, what type of data is involved, and security during transmission and storage. To ensure consistency from vendor to vendor, institutions should create form language for acceptable practices that can quickly be added to proposed agreement.

8. Updates. Your institution should be able to obtain updates from the vendor about its condition, including financial and IT. Contracts should spell out the availability, form and cost of any updates. Know what you want to review and how you want to receive it and get it in writing.

9. Security issues. Contracts should spell out how security incidents are handled including how quickly your institution will be notified, what form notification will take and what data will be available. Require a root cause analysis of incidents along with the ability to terminate.

> Never let a vendor's reputation or size substitute for actual testing.

A Simple Solution

The framework is an essential tool for identifying and mitigating the risks of third-party vendors, ensuring that vendors don't create weaknesses in an institution's BCP. Yet it is still a complicated process. There are standardized policies and procedures to write to ensure thorough, consistent results. There are contracts to negotiate and monitor and test results to track and analyze. There must be communication between business continuity and vendor management. Failing to do any of these can create gaps in an institution's business continuity plan—something that may only be discovered when the plan is in action and it's too late to fix the problem.

It's important to find a solution that addresses these concerns, ensuring an institution can harness is collective knowledge and resources to create a cohesive plan that integrates regulatory guidance and best practices.

Business continuity and disaster recovery are full of unknowns, but one thing an institution needs to know for sure is that it has a properly drafted, executed and tested business continuity plan—and that its vendors do too.

Ncontracts® is a leading provider of risk management software and services to financial institutions. While we started with our industry-leading vendor management platform, our portfolio offerings have evolved to feature enterprise risk management, business continuity risk management, compliance management, findings management, and cybersecurity management. More than 600 financial organizations use Ncontracts to manage risk more efficiently and effectively using our integrated suite of software and services.

CONTRACTS
The Upside of Risk

(888) 370-5552
info@ncontracts.com
www.ncontracts.com