Diligent

How to Manage Third-Party Risk During a Crisis

Table of Contents

Forced to Improvise Without Warning

When COVID-19 became a pandemic in March 2020, companies everywhere were forced to improvise without warning. Office workers had just a few days' notice to pack up their desks and make the move to a fully remote work environment. In many cases, IT teams were stuck setting up remote infrastructure using outdated systems and processes. **A survey of IT managers** published in Bdaily, a UK business news site, reported that 37% of IT leaders said that employees didn't have the right tools to work from home when such policies were initially introduced.

37%

of IT leaders said that employees didn't have the right tools to work from home.

Third-party risk management is an important part of your business, but when you're forced to improvise with new tools and ad hoc remote work environments, it can be difficult to maintain and manage adequate risk management processes.

The Focus On Third-Party Risk Has Increased

Third-party risk management includes a wide scope of risks, which may include strategic risks, operational risks, reputational risks and cybersecurity risks. Assuming your vendors' risks can also result in a significant impact on your own organization: **50% of respondents to a Deloitte survey** said that the costs of a vendor failure to their companies had at least doubled within the last five years, and 30% predicted a fall in company stock price in excess of 10%. And even before COVID-19, many enterprises were doing a poor job of preventing third-party risks: per the survey above, 84% had faced at least one third-party incident within the last three years.

84%

had faced at least one third-party incident within the last three years.

In light of the pandemic, many compliance leaders are concerned about a variety of increased third-party risks. **A Gartner survey** found that 52% of compliance leaders are most concerned about cybersecurity risks, although smaller portions (10% each) are most concerned about bribery and corruption, privacy, fraud and ethical conduct. It's become crucial for compliance leaders to evaluate their current systems to ensure that they have a highly automated and foolproof process for managing third-party risk throughout the entire vendor life cycle, from procurement to onboarding to finance and auditing.

The COVID-19 pandemic came with minimal warning, but it won't be the only crisis your organization is likely to face. This eBook looks at how organizations can quickly pivot and build the right processes to maintain a secure third-party risk management profile when the unexpected occurs.

How the Sudden Shift to Remote Work Has Impacted Organizations

Businesses and government organizations build and rely on long-term plans—they're not used to sudden shifts in how they function. But that's exactly what happened when COVID-19 struck. **PricewaterhouseCoopers found** that, while only 39% of corporate offices had employees work remotely at least once a week prior to the pandemic, 77% of them did during the crisis, with most employees shifting to full-time work-from-home environments—which may lack the communication tools and security features that they were used to in the office environment.

This lack of foresight can lead to numerous types of vulnerabilities for these organizations. **A Science Applications International Corp (SAIC) survey of C-level federal executives** discovered that 75% found it extremely or somewhat difficult to detect fraud, waste and abuse during the pandemic, and that 74% found it extremely or somewhat difficult to protect government systems from cyberattack during the pandemic.

75%

found it extremely or somewhat difficult to detect fraud, waste and abuse during the pandemic, and 74% found it extremely or somewhat difficult to protect government systems from cyberattack during the pandemic.

How to Manage Third Parties

While some of the difficulties managing risk likely come down to a lack of communication or reduced oversight with regards to internal employees, much of the increased risk level is likely due to third-party vendors. **The Ponemon Institute found that the average company shares their data with 583 third-party vendors**, with Fortune 100 firms using tens of thousands of external vendors.

These vendors are likely experiencing disruptions to their own business processes, causing more potential for errors, fraud and security risk. Moreover, your business may have difficulty following its standard protocols for vendor risk management during the pandemic, so your managers may not have the checks and balances in place to catch the issues that they might discover in the corporate office setting.

When this happens, it's important not to panic or pass blame. Don't start by auditing your critical vendors, or outsource your worries to your contractors. Instead, take a proactive and empathetic approach. Focus on improving your communication with all of your vendors across multiple channels, and on validating the completion and accuracy of critical third-party inventory. Take stock of all of your risk management processes, and identify the gaps in how you currently operate. While the pandemic has likely caused huge business interruptions, it also poses an unprecedented opportunity to optimize your organization's risk management posture for the foreseeable future.

It's clear that organizations need to focus on quickly making shifts in their processes to safeguard their third-party risk-management practices after a disruption in their standard operating procedures, whether as a result of the pandemic or another unexpected crisis. Here are some ideas for improving your risk management practices when a crisis hits, and for ensuring that you'll maintain strong safeguards that will help your business stay protected in the years to come.

Step One: Build a Third-Party Risk Management Framework

Start by building out the specific dimensions you'll be evaluating in your third-party risk management strategy, and determine the benchmarks you'll use for measuring success around each dimension. You can use this to build out specific policies for all lines of business that will be used to set standard protocols, measure compliance and identify trigger points for further action.

For example, you should build a detailed assessment process for standard vendor-related documents—such as policy or procedural manuals, regulations, service level agreements (SLAs) and contracts—along with a process for feedback and correction requests if vendors do not meet your standard compliance requirements.

Once you've completed a full inventory of potential vendor risks, you can build a scorecard that you can use to assess your vendors against various criteria. For example:

- What is the vendor's credit rating?
- How many subcontractors does the vendor use?
- What cybersecurity measures do they have in place?
- Does the vendor have its own comprehensive crisis management plan?

Make sure that you have protocols in place for continually grading each vendor on key criteria, with policies in place for escalation when specific trigger actions occur.

Step Two: Segment and Monitor Your Vendors Accordingly

Once you've taken inventory of all of your vendors and conducted a scorecard-based risk assessment, it's important to segment them and allocate resources to monitoring their risk and compliance, based on key criteria.

For example, large vendors that provide knowledge, work or materials may play a crucial role in your company's infrastructure, and may require specialized onboarding and ongoing compliance assessment resources. Smaller vendors that only provide occasional services may be served by automated resources that track their compliance across various factors.

It's important to take account of all third parties that your company engages with, even if they're not granted access to secure data. While cybersecurity threats and financial fraud are risks with many partner companies, even a casual association with another company may lead to reputational risk if the relationship is not managed and monitored properly. Make sure you have access to ongoing data analysis that will help you to immediately identify any potential red flags with a vendor or third party in your company's network.

Step Three: Develop Ongoing Risk Assessment Monitoring Practices

In light of a crisis like COVID-19, it's imperative to focus on clear communication and transparency with your third-party vendors. Be proactive in developing ongoing risk assessment monitoring protocols that are tailored for each vendor's risk level, based on company size, level of interaction with sensitive data, and other criteria within your framework.

While risk assessment is important during an initial onboarding stage with each new vendor, ongoing risk assessment is also crucial. **A Gartner survey reports** that more than 80% of legal and compliance leaders said that third-party risk factors were identified after initial onboarding and compliance efforts.

While you should conduct a full risk assessment with each vendor at the onboarding stage, you can also identify trigger actions for further compliance assessments (e.g., quarterly review, credit monitoring alerts, new technologies). Depending on the size and involvement level of the vendor, some vendors may be able to complete initial self-assessments, while others may require dedicated resources. If a trigger action occurs, your risk management team can triage based on the type of action and prioritize those that need immediate action, or request further information from the vendor. From there, you can build an action plan that assigns next steps to stakeholders based on your findings.

Step Four: Invest In IT Tools to Manage Your Workflow and Automate Your Processes

During crisis situations that require employees to work remotely, you're not likely to have the same level of personal interaction and accountability that you would within a corporate office situation. That makes it critical to evaluate and build the right technology stack to oversee your risk management process through largely automated technology, with action items getting routed to relevant stakeholders based on set triggers.

Your organization needs to build an approach that focuses on the end-to-end risk management life cycle. This includes:

- Speeding up vendor onboarding and classification
- Cutting down on manual tasks with automated risk-based control assessments, including evidence collection, in one centralized repository
- Managing contracts with convenient workflow and signoff
- Using automated workflows, notifications and escalations to ensure nothing is missed

The tools you choose should not simply expedite your processes—they should offer continuous monitoring around metrics tied to various forms of risk, including cybersecurity, operational, fraud and reputation risk. Your analytics tools should draw from vendor-supplied data (i.e., onboarding questionnaires), your proprietary data and third-party data streams such as financial intelligence feeds, security ratings and credit ratings.

Crucially, your technology stack should include the capacity for real-time risk reporting, so that relevant stakeholders can be alerted and compliance or security issues can be prioritized immediately based on the level of action needed.

By setting up a detailed framework in advance, lower-level action items (such as requesting updated compliance documents) can be automated, saving your employees' time to focus on resolving more critical issues that require communication and care. A robust technology stack will make it easy for them to understand what the issues are, and what needs to be done to resolve them. It will mitigate the risk of serious issues like cybersecurity breaches and financial errors being overlooked, causing massive losses and reputation damage to your enterprise.

Preparing for the Future

Pandemics, natural disasters, political upheaval and other unexpected events all have the potential to cause chaos for your enterprise—but by hedging against uncertainty with clearly laid-out plans and processes, you'll be far better prepared than your competitors to weather whatever storms may come your way.

By building comprehensive processes and policies for procuring, onboarding and managing your third-party vendors and using cloud-based technology that can be securely accessed from any remote location, you can give your compliance managers the right tools to easily monitor and triage potential risks as they come up. Your solution should use a combination of vendor-provided data, proprietary data and real-time monitoring to provide access to dashboards with robust analytics, along with alerts for issues that need to be resolved and automated trigger actions for those that don't require human intervention.

When you're operating in a crisis, you shouldn't need to focus your resources on checking up on your vendors. By putting a solid framework and strong processes in place now, you can protect your organization and conserve your team's time and productivity, no matter what the future brings.

About Diligent

Diligent created the modern governance movement. As the leading governance, risk and compliance (GRC) SaaS company, we serve 1 million users from over 25,000 customers around the globe. Our innovative platform gives leaders a connected view of governance, risk, compliance and ESG across their organization. Our world-changing idea is to empower leaders with the technology, insights and connections they need to drive greater impact and accountability – to lead with purpose.

For more information or to request a demo, contact us today:
Email: info@diligent.com | Call: +1 877 434 5443 | Visit: diligent.com