THIRD PARTY RISK MANAGEMENT RESPONSE TO COVID-19

Alpa Inamdar
Head of Third-Party Advisory
BNY Mellon Group

With 20+ plus years' experience, for the past 13 years, I have worked in the financial industry for firms including Société Générale, Goldman Sachs, and BNY Mellon. I am currently Head of Third-Party Advisory at BNY Mellon Group and my role is to ensure that, across all 22 lines of business, we are successfully managing our third-party risk. Whether in regard to asset servicing, asset management, legal, finance, compliance, or more, we consider the operational, financial, geopolitical, compliance, and economic risks, among others. The Third-Party Advisory's role is to ensure that all these business areas are compliant with the third-party governance policies and procedures. I am also a member of Shared Assessment, who are industry leaders in third-party risk assessment and certification. I sit on the Risk Board, leveraging peer-to-peer networking on third-party governance across different industries, not just financial.

> ***"During COVID, we experienced supplier shortages, from the shortage of toilet paper to ensuring the right suppliers were providing a service to make sure that transactions or proxy statements could go out on time. It has really brought this topic to the front of senior leadership agendas."***

How have you seen the events of 2020 impact third-party risk management?

In the past, we have always focused on a single event or have considered risk as linear, impacting a specific industry – until COVID, which has impacted all locations and all industries. One thing that COVID highlighted for us in 2020 is that third-party risk management is an important and critical element of long-term success. It has never been so heightened or such a foremost agenda topic for boards or executives across the regulatory landscape; this is the case across all industries and all regions. During COVID, we experienced supplier shortages, from the shortage of toilet paper to ensuring the right suppliers were providing a service to make sure that transactions or proxy statements could go out on time. It has really brought this topic to the front of senior leadership agendas.

One thing this crisis has helped people to learn is that it is so important to know who your critical vendors are and how they are monitoring their risk – for example, their location, the type of contracts you have with them, the infrastructure they currently have, and perhaps most importantly, the resources and services they provide to the organization. Given that so many are now working from home, the infrastructure may not be able to deal with this additional capacity, as demands and systems are being utilized beyond a capacity we never considered. From an industry perspective, we had to ensure we had enough laptops and RSA tokens available. We also had to alter our service-level agreements (SLAs) because for most of our vendors, especially those in locations such as India or Poland, we did not have a clause that permitted them to work from home. We had to work with the legal team to update our SLAs and add in provisional clauses from a legal perspective. In the past, we would go to each specific vendor at their location for an on-site assessment to ensure they were following the correct due diligence. These had to be conducted virtually, as many of them are working from home. The challenge was how to still understand the risk and make sure that people are abiding to the policies and procedures, whilst feeling >>

comfortable to be able to effectively monitor risk. These are some of the key events that took third-party risk in a very different direction.

What for you are some of the lessons learned from responses to the global pandemic?

We learned a lot of lessons or best practices throughout COVID; not least, the extent to which we understand our critical vendors. We conducted a survey with all of our critical vendors in light of COVID to understand if they have the right infrastructure and resources in place, and whether this could have an impact on services. We found that we did not have the latest contact details for many of them, or that the relevant person was no longer at the firm or had changed location. So simply ensuring you have the latest contact details is crucial, alongside monitoring whether vendors remain classified as a critical vendor. Things changed very quickly in 2020; we needed to continually assess the situation, so those steps were lessons learned.

The other key lesson we learned is that we had to change our operating model to incorporate building a workforce for the future. As an industry, the financial services workforce has not really had the opportunity to work from home. For roles such as traders, remote working was not something that was considered acceptable. Given the pandemic, we had to change that process and update our operating models to ensure that people are able to work from home. At the same time, we had to make sure we used the right protocols and tools to mitigate any risk, including increased phishing attempts, cyber risks, or simply ensuring that computers had the latest updates available. Many company controls were designed around staff working in a company-managed facility; however, we now had people using confidential data in an unsecure environment. It has therefore become increasingly important to optimize technology and automation. We have learned that what worked 10 years ago will not work today. We have to manage this risk and use technology to do more predictive analysis for us.

In this regard, one of the things we are starting to do is look at the trends of some of our vendors over the last few years; things like divestures, any significant change in their financial statement, their balance sheet, whether they have lost any key talent, etc. All of these could be indicators that the company may not be doing well. Rather than being reactive, how do we make sure we take this data and use AI to help us predict vendor relationships? Methods that have been used in market and credit risk for decades, such as continuous monitoring and forecasting, are now being applied to the supply chain. Although we will still need the human element, I think that technology and automation will be used much more in this instance to help us achieve this goal.

Another key lesson learned is the importance of reviewing the resilience of pandemic plans and making sure that they are up to date. As on-site visits are no longer viable and due diligence has moved to a tabletop exercise, it is important to ensure we are comfortable with the data available, or the frequency of pandemic plans may need updating.

Another process to review is that of location and concentration of vendors. Previously, little focus was given to location; however, given the widespread impact of the pandemic, we need to review vendor locations and concentration in certain regions – for example, EMEA, Asia, or the US – and the risk this could pose to the organization. Also important is making sure that policies and procedures are updated to reflect the current working environment. As institutions become more familiar with the risks associated with working from home, it is important to update policies to incorporate clauses that reflect it and make changes to areas, including alternatives to on-site assessments. It is important to ensure that contract reviews happen more periodically, especially those that are evergreen, to understand the impact on our function and ensure that an open channel of communication is maintained. In the end, it is vital to have an open channel of communication with vendors to understand their strategy and roadmap.

> *"Given the pandemic, we had to change that process and update our operating models to ensure that people are able to work from home. At the same time, we had to make sure we used the right protocols and tools to mitigate any risk, including increased phishing attempts, cyber risks, or simply ensuring that computers had the latest updates available. Many company controls were designed around staff working in a company-managed facility; however, we now had people using confidential data in an unsecure environment."*

Why is continuous monitoring a critical function of third-party risk?

Continuous monitoring is a critical step towards moving away from manual questionnaires and single point-in-time processing. Given the rapid changes that have led to the current environment, these just do not work anymore. We usually complete a risk assessment and carry out due diligence when onboarding or terminating a vendor or client, based on whether they are critical, high, moderate, or low engagement. For critical, we conduct it every year; for high to moderate, we do it every two years; and for low we do it every three years.

Given the current landscape, static data is insufficient; we need dynamic, agile risk intelligence. Continuous monitoring is going to be vital in providing real-time alerts to notify of the risk for each vendor. Based on these alerts, we will need to do additional due diligence and investigate what domains have been impacted, or data triggered. We cannot rely on the information of a vendor that we did due diligence on a year ago and assume that nothing has changed. Continuous monitoring plays a critical role in the ability to assess and classify criticality of vendors. Developing and maintaining continuous intelligence monitoring and reviewing data will significantly assist in understanding risk across the vendor portfolio.

What are some of the challenges and considerations with continuous monitoring?

We talk about continuous monitoring as a crucial step for an organization to identify and to detect risk. But at the same time, there is a risk of information overload. For example, if you receive a high number of alerts, what do you do with them? The expectation is to notify and understand your risk, but what do you then do to resolve or mitigate it? Having proper escalation processes is going to be crucial in >>

ensuring the right people receive the right information in a timely manner. Implementing strong governance is also important to evidence resolution of an issue. It is not good enough simply to identify the issue; you must also be able to provide evidence to regulators, executives, or the board demonstrating how it was resolved. It is also worth considering that some of the information might be inaccurate of falsified. How do you differentiate between real data and the outliers? How do you manage that data and track it? Data that has been curated eliminates the uncertainty and streamlines the response process.

The other challenge, especially for tier one and tier two organizations that may have a lot of legacy systems and software with multiple disparate systems, is how to make sure that the continuous monitoring data set triggers an alert and gets flagged. Is there a consistent process for measuring that risk scoring? Continuous monitoring systems can have very different criteria and approaches for measuring risk; are all systems in the organization following the same process? I would honestly say that in most companies they are not, which is one of the key challenges we are facing regarding continuous monitoring.

How have regulatory changes on third-party governance impacted third-party risk management programs?

Regulators are getting more and more robust and requesting that the industry has a comprehensive inventory of third parties. However, it is not good enough just to have a comprehensive inventory; the question now is, how do you manage that risk? Regulators are taking it one step further and requesting an inventory of fourth and fifth parties, and expecting an understanding of the protocols, controls, and infrastructure to manage risk.

In addition, given that information is now heavily cloud-based, the EBA and PRA are asking for a cloud registry to better understand the risks to an organization, the potential impacts, and which vendors are using which cloud provider. The regulators want to understand what kind of disciplined governance process you have, how you are managing the business, and how you are managing third-party governance functions, as well as areas not limited to procurement, compliance, technology, and operations. So, not just one function but, as an organization, how is that risk being managed across all the different lines of business? In addition, across EMEA, a big focus is being put on inter-affiliate entities and understanding the risks associated with them, as a result of regulations. No matter how big an organization, it is vital to ensure a consistent approach across the entire business to ensure a framework is in place that makes regulators feel comfortable that not all responsibilities are being outsourced, but are being managed in-house with the right structure and categorization.

What are some of the social responsibility and ethical considerations?

More and more companies are moving towards corporate social responsibility and environmental social governance (ESG) disclosures. They are now looking at, and becoming more conscious of, their carbon footprint. We've come a long way in this regard, and it is very important as an organization to consider diversity when onboarding vendors; matching locations, as well as what they do to support the broader society.

This is also important from a reputational perspective. Does the vendor enhance reputation or bring reputational risk to the organization? When we go through the process of onboarding vendors and assessing them, we need to consider and collect evidence regarding their compliance with modern slavery acts, forced labor laws, and human trafficking laws. It is important to understand the steps vendors are taking to comply with such laws and review evidence before signing any agreement. We also analyze the proxy data set to ensure we feel comfortable to stand behind a vendor. It is not good enough that they provide a service; we take a more holistic view and consider their reputation, and how they are helping society. I think more and more we will see reputation and resilience as critical factors of the overall third-party program.

What do you see as the way forward for third-party risk management?

Third-party risk management is going to gain a lot of visibility as a result of COVID-19, becoming more evident in 2021. I expect organizations will be held more accountable for their third-party risk management. Board-level involvement will become more common because of the cybersecurity risk. However, the risk landscape has evolved much wider than this, and now it's not just about the cyber risk. With much of the workforce still working from home, cyber risk cannot be viewed in a vacuum; operational risks more broadly have also increased. For example, if an organization has a system failure, how quickly is it able to come out of it? There are heightened financial risks, too. A lot of companies will be unable to survive the economic impacts; do your vendors have good financial stability and a strong capital and balance sheet?

Before, organizations were focused on cyber risk but there are now at least nine different risks for which firms will have to be accountable: operational, financial, reputational, compliance, geopolitical, cyber, information security, ESG, and privacy. Recently, we have seen an increase in data breaches, not least the FireEye case, which impacted many. I would expect to see more of these moving forward. As such, organizations will need to be more proactive than reactive because they will not be able to sustain their position without using some of this information and intelligence to carry out predictive analysis. There is more to come in 2021, but I believe that third-party risk management will be the foremost upfront agenda for regulators, as well as for stakeholders and the board.