New perspectives on Third Party Risk Management

Navigating through the COVID-19 Crisis

Summary

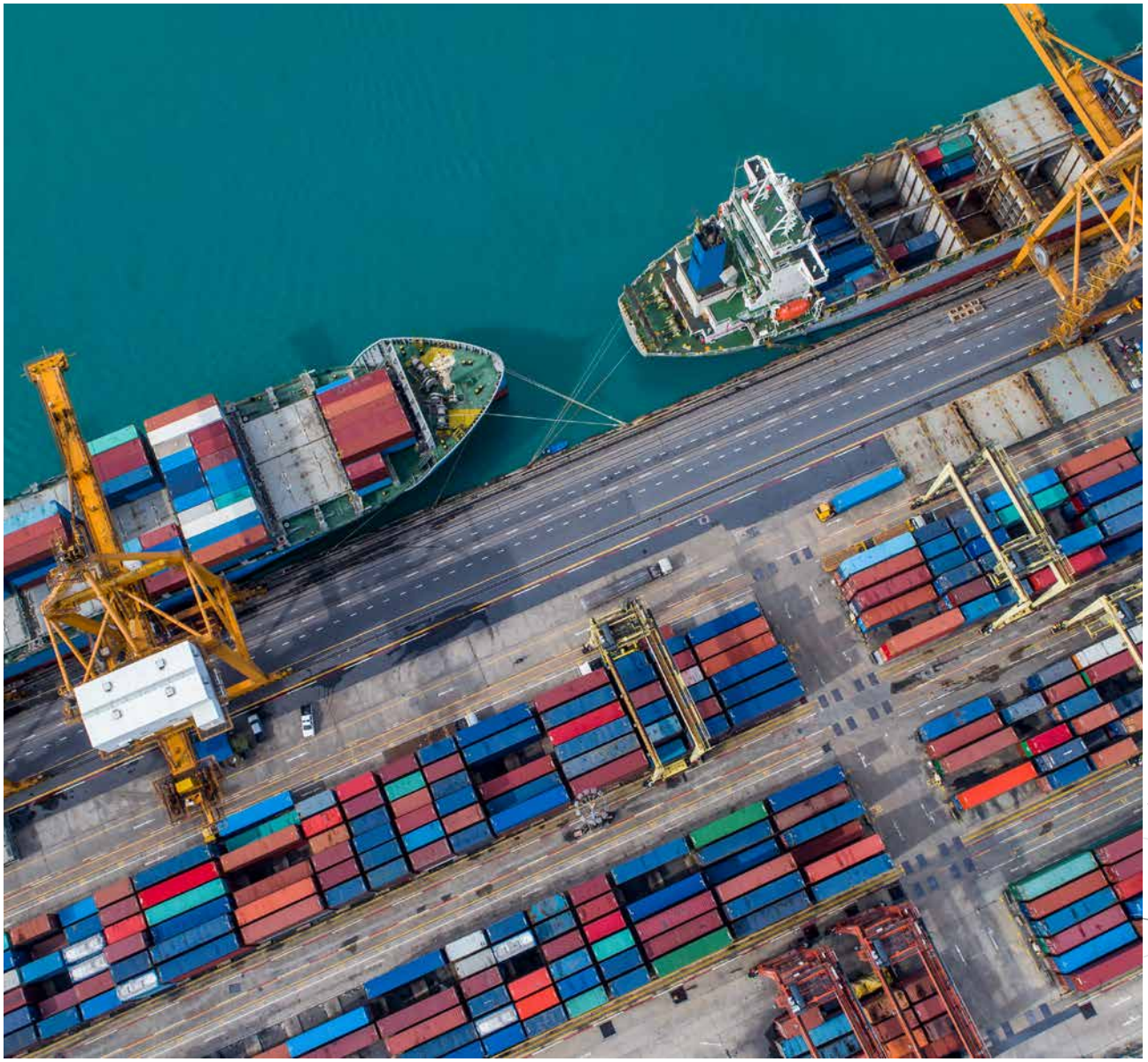
Companies are currently hit by the COVID-19 crisis and need to respond promptly to ensure business continuity, especially when relying on third parties. If companies are slow to react, there will be an adverse impact on their operations and overall business performance, which can eventually result in adverse media. This article will help you to manage the new challenges and risks in an efficient and effective way. Based on market insights, our focus will be on the following key challenges:

- Which risks require increased attention given the current situation of the COVID-19 crisis?
- How do you identify critical third parties which are impacted by the COVID-19 crisis?
- What needs to be done to properly assess critical third parties and to initiate mitigating measures?
- How can you secure your employees and ensure that the increased level of workload in the TPRM area can be performed?
- Which key role does a TPRM technology solution play in the COVID-19 crisis?

Including a COVID-19 crisis immediate action checklist located at the end of this document

pwc

Contents



I. COVID-19 crisis and the impact on third parties

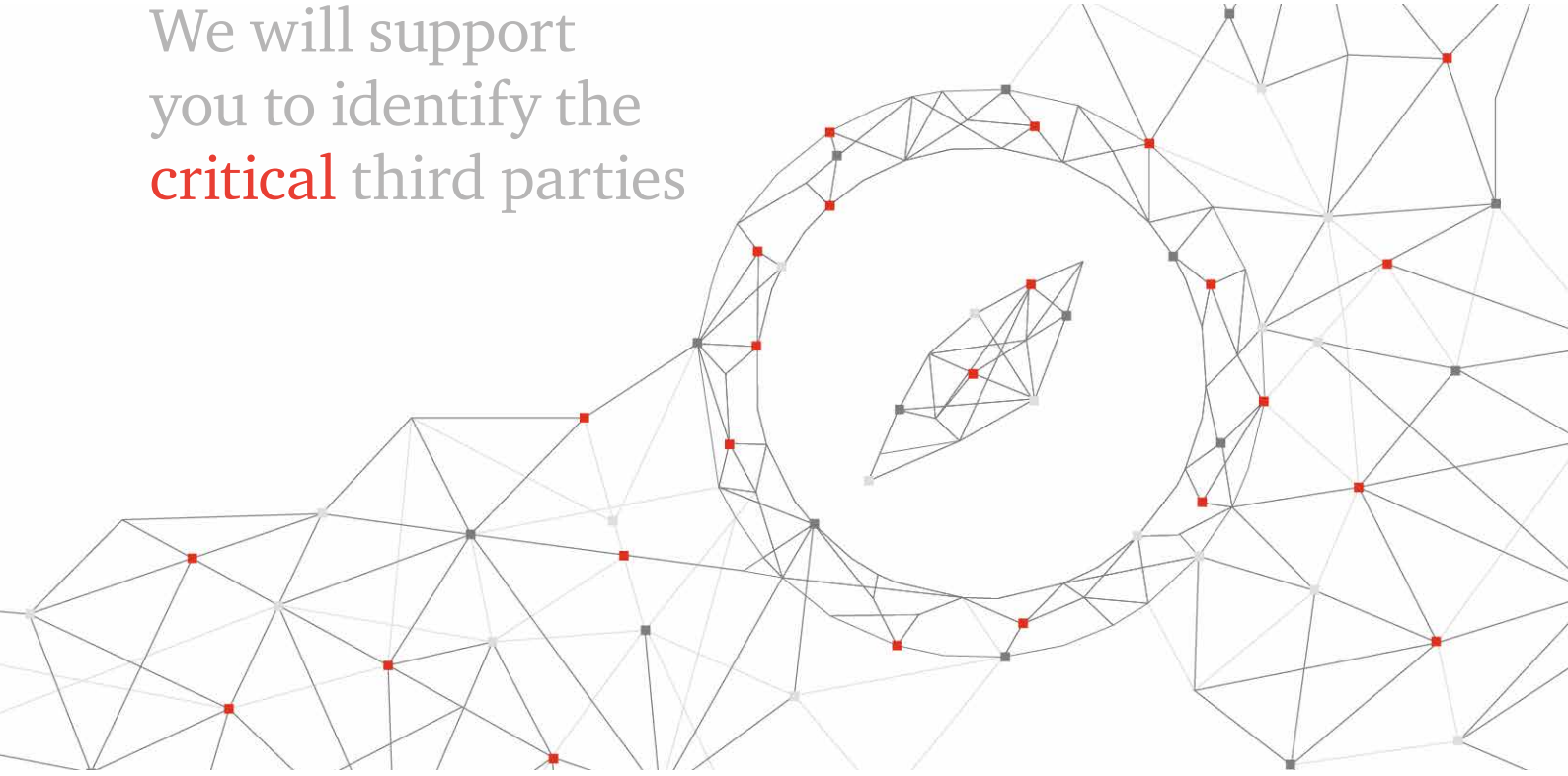
A survey by the Institute for Supply Management (ISM) shows that almost three quarters of all supply chains are undergoing interruptions caused by the Covid-19 outbreak.[1] This phenomenon is expected to intensify, as a growing number of countries are starting to be severely affected by the virus. As processes within corporations have become increasingly complex in the recent years, the discipline of identification, measurement and management of risks originating from outsourcing to third parties has never been more important.

Across different countries and industries, the COVID-19 crisis disrupts business as usual operations because a wide range of services are outsourced to external providers. Breakdowns and interruption in external services lead to significant damages.

Therefore, the COVID-19 crisis has stressed the importance of business continuity plans and is currently testing the effectiveness and practicality of such plans. Where the stability of the company's operational activities is set at the forefront, the increasing reliance on third party service providers is putting companies in a challenging situation. Whether it involves critical parts of the supply chain or revenue sharing activities, an existing third party risk management (TPRM) framework needs to be adjusted to account for extreme events, such as the COVID-19 crisis. This article seeks answers to such questions and provides practical insights based on recent experiences and insights.

- How can companies manage third party risk whilst navigating through the COVID-19 crisis?
- Which third party risks require extra attention?
- What should a TPRM Crisis Playbook include?

We will support you to identify the critical third parties



1 https://www.instituteforsupplymanagement.org/news/NewsRoomDetail.cfm?ItemNumber=31171&SSO=1

II. Key risks of the crisis impacting your company

In “business as usual” times, procurement and third party risk management teams carry out due diligence and ongoing monitoring of these third parties, such as vendors, outsourcing partners, and others across a broad range of risk domains. The challenge which comes with the COVID-19 crisis is that certain risks are now more relevant than others, and the focus of the due diligence assessments might not be sufficient anymore.

Business continuity risk

This is one of the major risks in situations like a pandemic outbreak, and addresses the capability of vendors to continuously provide agreed products and / or services. Compared to “normal” times, where the focus of the risk assessment is on the review of the continuity plans, the target now is to understand if these plans were executed and whether any negative impacts can be expected.

Information security risk

These risks are significantly greater in times of a pandemic outbreak, especially because companies have mandated their employees to work remotely from home. This increased the information security risk, due to the widespread use of private networks and devices, and also increased sharing of digital information and higher dependence on third party service providers (e.g. remote desktops).

Third party types in scope

In light of the COVID-19 crisis a special emphasis can be placed on the different third party types. Looking at traditional suppliers, the situation indicates that business process outsourcing and IT outsourcing of critical functions can be a threat, especially when the supply chain is being disrupted, for example by split operations, reduced work force, decreased productivity, inability to access the office or travel restrictions. An assessment per supplier category can shed light on particular risks that are more relevant within a specific category. Hence, a categorised approach can be more effective in terms of identification, assessment, remediation and monitoring of such risks. For example, inability to access the office can have a substantial impact on critical business processes provided by a third party, including quality and timeliness.

A robust third party risk framework considers the management of all third party types. Companies still struggle with the assessment and monitoring of special third party types (e.g. affiliates, brokers, law firms, regulated entities). The risk management of such third party types might not fit within the traditional framework (*PwC One Size doesn't fit all: Managing special third party relationships*[2]). Therefore, the COVID-19 crisis can pose additional pressure on the management of special third party types. In case decentralised processes exist for special third party types, companies need to review and potentially adjust these to deal with the characteristics of a pandemic outbreak (ensure business continuity, performance etc.).

2 https://www.pwc.com/us/en/industries/banking-capital-markets/consumer-finance/library/tprm-special-categories.html

Performance & quality risk

Supplier performance and quality assurance remains a challenging task in times of uncertainty. The delivery of critical services can be hampered by the performance of the supplier, which due to various factors, (e.g. global supply chain, fourth parties and operational challenges), will be negatively impacted. SLAs that are designed to function under normal circumstances might come under pressure and need to be reviewed.

Geopolitical risk

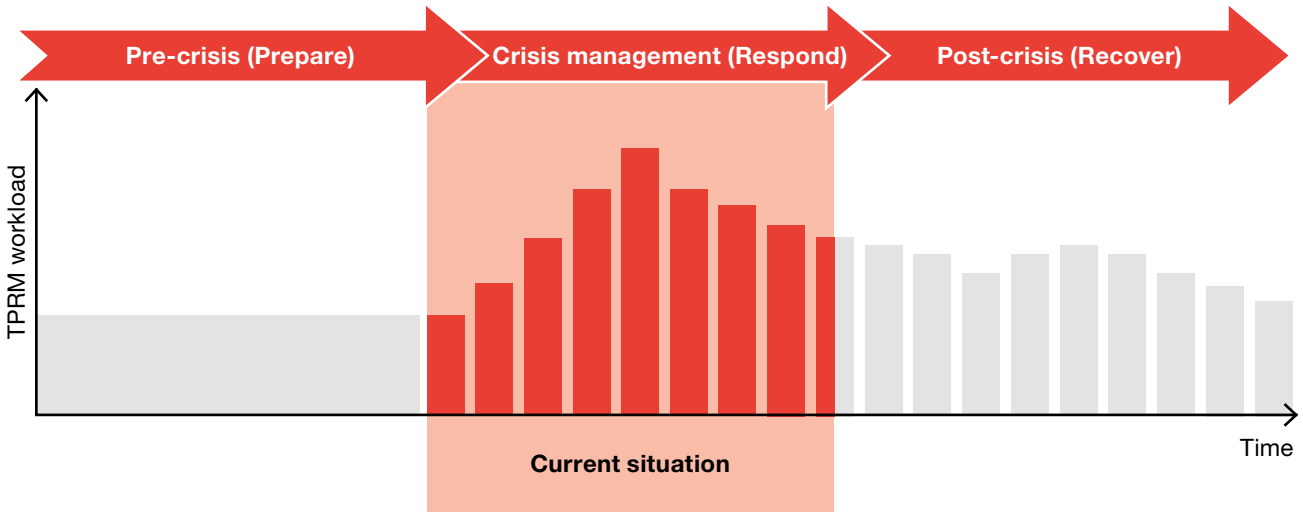
Geopolitical risk requires extra attention, which we are learning from the COVID-19 crisis. Countries are taking extreme measures to cope with the current situation, such as in-country lock downs, travel bans, import/export restrictions, social distancing etc. Differences in national or federal policy response can pose additional third party risks, especially with vendors located in high risk areas (e.g. a country with high infection rate/political risk).

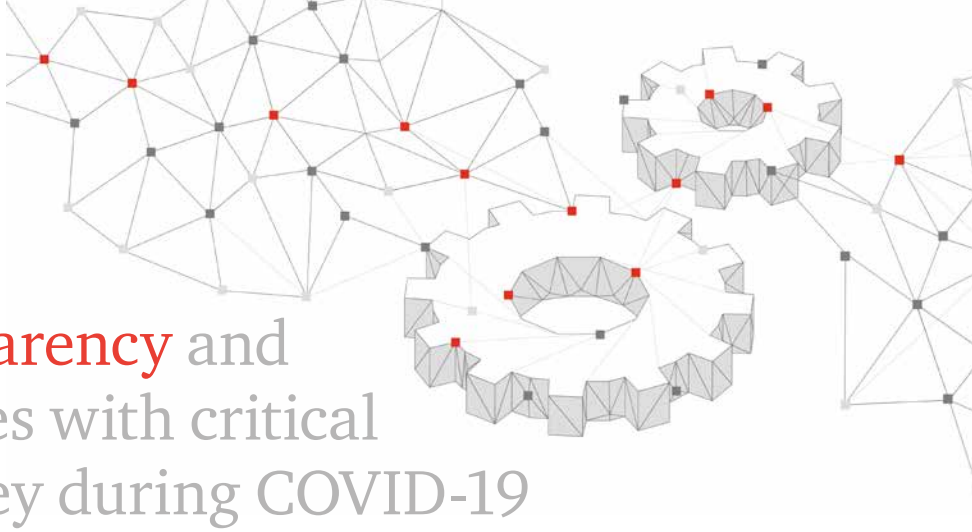
Fourth party risk

Fourth party risk management was already a critical topic before the crisis because transparency of the vendor's supply chain is often lacking. It is important that fourth parties which are providing critical services are also risk assessed like third parties, especially regarding to the above mentioned risks.

III. Navigating through the crisis with a TPRM Crisis Playbook

With events such as COVID-19, third party risk organisations are facing challenges that have the potential to cause significant business disruptions, which can generate extensive media coverage. Therefore, it is necessary to have a proper TPRM Crisis Playbook, which is designed to provide clear instructions such that the negative impact on the business can be limited. Third party crisis management starts before the crisis with the pre-crisis phase, followed by the crisis management phase, and ending with a post-crisis phase.





Trust and transparency and regular exchanges with critical third parties is key during COVID-19

Pre-crisis (Prepare) → Crisis management (Respond) → Post-crisis (Recover)

Pre-crisis (Prepare) phase

In this first phase, the target is to identify different types of crisis scenarios which might impact the organisations and, in this case, especially the third party risk management organisation. The types of crises are constantly growing and include natural disasters, technological crisis, terrorist attacks/man-made disasters, or a pandemic. Preparation involves creating the crisis management plan (CMP), selecting and training the crisis management team, and conducting exercises to test the crisis management plan and crisis management team

Best practice components of the pre-crisis phase:

a. Nominate a crisis management team with clearly defined roles and responsibilities
b. Define a crisis management plan which is updated at least on a yearly basis
c. At least once a year perform tests of the crisis management plan and team

Pre-crisis (Prepare) → **Crisis management (Respond)** → Post-crisis (Recover)

Crisis management (Response) phase

Since the COVID-19 crisis started all financial institutions are in the crisis management phase. Third party risk management organisations are suddenly exposed to new internal and external risks and challenges. In the best case scenario, one of the pre-defined crisis plans is matching with the actual crisis. In the COVID-19 crisis, this was typically not the case and thus adjustments are needed to incorporate its specific challenges.

Based on conversations with different financial service providers we could identify companies which were more successful in managing these challenges than others. One of the most important success criteria was a regular interaction (via mail, call, video conference) with the critical third parties to create trust and transparency. Since currently all companies are more or less under pressure, open discussions and pragmatic solutions will strengthen partnerships in the future.

Other major differences between successful and unsuccessful responses to the crisis were linked to the selection of the crisis management team, the risk assessment process, the treatment of the internal employees, and the use of third party risk management tools. Key elements are outlined on next page:

Key element of the Crisis management (Respond) phase

Crisis management team

A strong crisis management team is one of the key components to successfully manage the crisis. To form a strong team, it is important to have the right people in the right position that suits their individual strengths. The purpose of a crisis management team is to lead and manage individuals, communicate important information to all departments, and analyse the problem and potential damages. Normally the heads of the procurement and third party risk management organisation should be in the crisis management team.

Beside the crisis management team, a crisis committee is required where key representatives align on a regular basis (even daily) to discuss relevant topics, such as the development of the overall situation (industry / country specific reports) or specific third party relationships which are, or might be, at risk. The committee should be empowered to agree on mitigating measures or actions. The following key stakeholder groups are typically involved in these discussions:

- Vendor risk managers/procurement (crisis management team)
- Senior business representatives which are responsible for managing the vendors
- SMEs of the different risk functions (cyber, legal, compliance, BCM etc.)

Risk assessment process

Third party risk assessments are typically done before the start of the engagement and repeated on a periodical basis to ensure that changes in the risk of the supplier, the provided product, or the service are monitored. The risk assessment which occurs during the crisis is different because, as mentioned in Chapter II, specific risks can be identified, which is what we observe with the COVID-19 virus. The target now is to achieve more insights on the ability of the third party to provide the agreed product and services on a continued basis. Given companies today leverage a large number of third parties, the risk assessment should be risk based and tailored to the most critical third parties.

Therefore the following 3 step approach is commonly used.

1. Identification of critical third parties	• One common way in the third party risk management is to assess each new engagement and respective vendor and determine the criticality on factors like business continuity relevancy • Important: Defined criteria for criticality should be reviewed and enhanced by additional key risk indicators tailored to the specific impact of the COVID-19 crisis
2. Assessment of the critical third parties	• Target of the risk assessment step is to verify and determine the probability that the respective vendor is not able to provide the agreed product/service on a continues basis • Different data and information should be leveraged for the assessment, such as – Self certification provided by the vendor during on-boarding (continuity plan, policies etc.) – Publicly available information or data provider for negative news/sanctions screening – Specifically tailored/updated due diligence questionnaires/self certification for the COVID-19 crisis • Especially the tailored due diligence questionnaire can be leveraged to close risk assessment gaps which were not checked in the initial on-boarding assessment • Finally, information are assessed and a risk rating is assigned to potentially trigger the next step

3. Identification of risk mitigating measures	• In this step of the process the crisis management committee has the task to review the critical third party positions and agree on next steps • The target is to define risk mitigating measures or to initiate a transition process into another solution: – Insourcing or – Execute a second vendor strategy or • In case no equivalent vendor exists, the outsourcing company might consider supporting the company e.g. financially.

In a crisis changes can happen at a very short notice. Therefore, a frequent monitoring and reporting across the vendor universe needs to take place on an ongoing basis to timely detect potential issues and to initiate respective actions.

Employee

Especially in a crisis, it is important to have the required workforce to manage not only the daily business but also the additional workload linked to the crisis activities (e.g. additional assessments, meetings, calls, coordination tasks). Employees are the most valuable source and need to be protected to ensure availability. Therefore nearly all companies advise their employees to work from home. However, in case the workload cannot be managed anymore companies should plan to leverage external support.

In case your business is supported by an external service delivery company which provides flexible resources, it is important to ensure that these resources are available and reserved. We often observe today pooled employees who are are in parallel leveraged by various other companies might not be available anymore.

Another challenge we see is that, especially in de-centralised third party risk management organisations, the low availability of risk SMEs (not located in the same reporting line) to perform certain risk assessments results in delays and subsequently increasing risks. Therefore, clear rules specifying availability need to be defined.

TPRM tool solutions

In the market today, we see that companies with a proper third party management tool are managing the challenges of the COVID-19 crisis in a much more efficient way. This is primarily because of a well-defined client life-cycle process linked with a structured assessment and a systematic documentation (e.g. of the due diligence questionnaires) on a contract and third party level. Based on the data collection, critical vendors can be timely identified by simply adjusting certain filter criteria on the third party universe.

As the execution of due diligence questionnaires is fully automated, and artificial intelligence can be leveraged to analyse results, the majority of the cases can be automatically pre-assessed by the system. Solutions which provide ongoing monitoring can be linked in via interfaces and determine, based on a matching algorithm, the probability that certain negative news will impact their third parties. Any identified issues are automatically tracked and managed by the system to ensure a proper mitigation including the respective audit trail.

Best practice components for the crisis management phase:

a. Have a proper crisis management team and crisis management committee in place
b. Perform re-assessment of the vendor universe based on COVID-19 crisis specific parameters
c. Safeguard your workforce to ensure availability (considerer leveraging external support)
d. Ensure that a proper third party risk management tool is in place

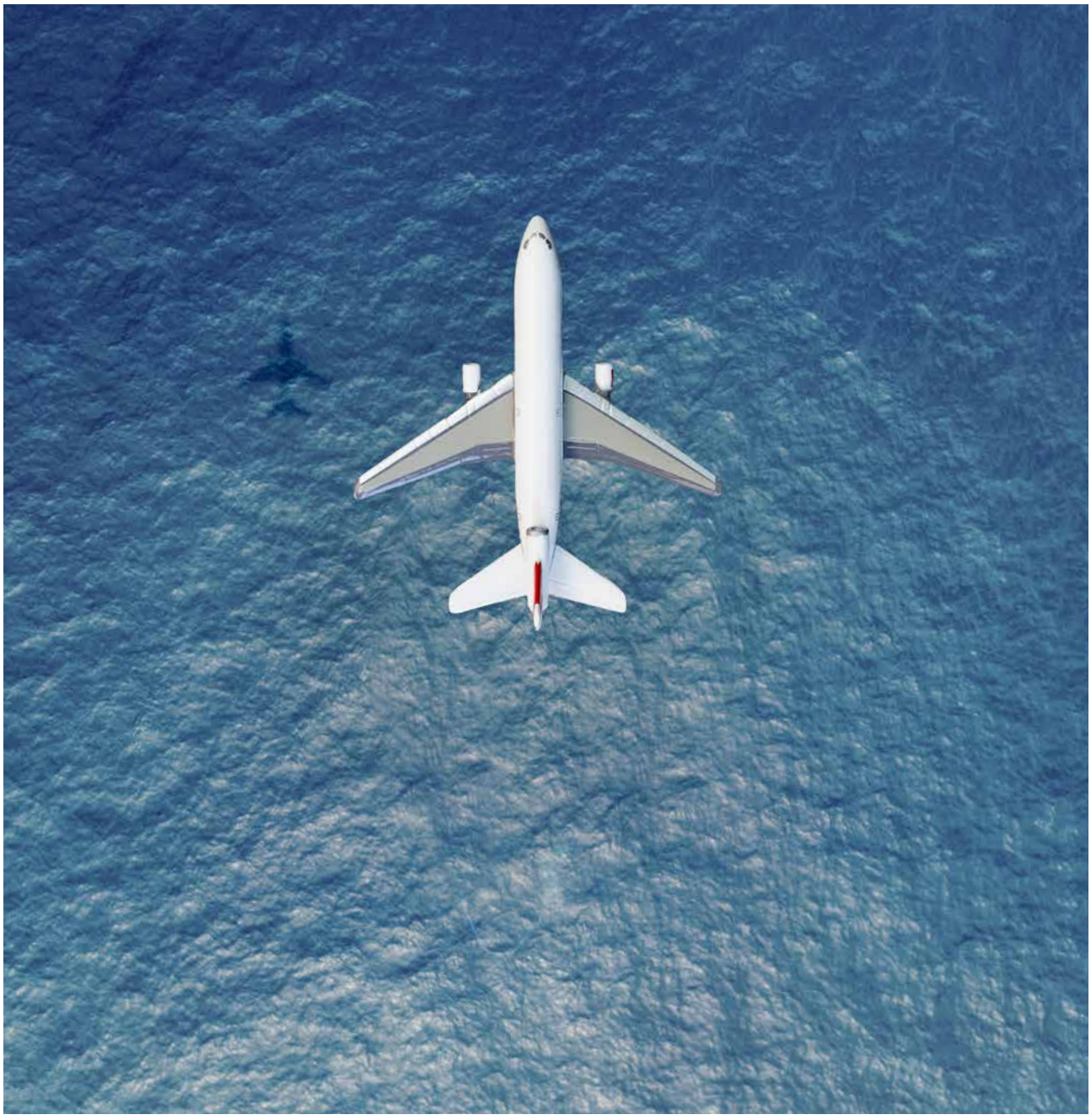
Post-crisis (Recover) phase

In the post-crisis phase the organisation returns to a business as usual state. The crisis is no longer the center of the management's attention. In this phase the company needs to review and update their recovery process, corrective actions, and/or investigations of the crisis. This includes tasks, such as the evaluation of the crisis management team and the crisis management committee, which should involve all key stakeholders with the target to improve prevention, preparation, and response for the next crisis.

Best practice components for the post-crisis phase:

a. Review and update the crisis management plan based on lesson learned

b. Perform an evaluation of the crisis management team and crisis management committee



IV. COVID-19 crisis immediate action checklist

The below COVID-19 crisis checklist was created based on the major challenges which we currently see in the market.

Topic	Check	Action
Crisis management team/Crisis management committee	Do you have a senior crisis management team in place to coordinate and enforce required actions?	Key members should be selected, such as the head of procurement/ TPRM.
	Do you have a crisis management committee in place with senior key representatives?	The Crisis committee team should nominate required members covering all relevant risk areas.
Risk re-assessment	Did you enhanced your criticality criteria and assessment approach for third parties by COVID-19 specific risks?	Enhance the criticality definition of your third parties.
	Do you have a tailored due diligence assessment questionnaire in place to assess COVID-19 specific aspects, such as the status of the third party's business continuity plan?	Define a questionnaire which is a) closing the gap between you basic assessment and the new risks by the COVID-19. b) Checking the current vendor regarding to e.g. the execution of the business continuity plan.
	Did you perform a re-assessment of the critical third parties by using the new criticality definition?	Execute a screening of your third party universe and perform a deep dive assessment.
	Are for all identified critical third parties mitigating actions in place?	Present each critical third party in the crisis management team and agree on mitigating actions and next steps.
Employees	Did you safeguard your employees and are they able to work e.g. remotely?	Ensure that the right actions are taken and that the infrastructure is available to continue working.
	Is the workforce sufficient to cover the daily business and the increased level of workload because of the crisis?	Consider and prepare for leveraging external resources on a temporary basis to breach the gaps.
TPRM tool solutions	Does your TPRM tool have sufficient capacity to handle increased volumes and features 'work from home' capabilities?	Ensure operational effectiveness of the TPRM tool, including when working from a remote location.
	Does your TPRM tool allow for regular crisis status reporting?	Define and setup the crisis reporting template.

We are looking forward to discuss with you a more detailed view on the individual actions which need to be tailored to your specific organisation.

Your contacts

Patrick Akiki
Partner
akiki.patrick@ch.pwc.com

Adam Mikulka
Partner
adam.r.mikulka@ch.pwc.com

Thomas Busch
Senior Manager
thomas.busch@ch.pwc.com

Urgyen Ponse
Manager
urgyen.ponse@ch.pwc.com

Martin Flisek
Manager
martin.flisek@ch.pwc.com

We would like to thank Garett Myers and Carlo Schmid for his contributions to this publication.