Thriving in the new reality

Novel approaches for third-party risk management (TPRM) in response to COVID-19

May 14, 2020

kpmg.com

May 14, 2020

KPMG

KPMG has broadly defined four phases for businesses to consider in response to COVID-19: Reaction, Resilience, Recovery, and the New Reality. Applied in the context of TPRM, these phases help businesses focus on the immediate and long-term actions that risk management should be taking to ensure third-party risks are identified, monitored, and managed—even in this unprecedented environment.

Reaction and Resilience

Emergency move to remote working models and rapid reconfiguration of third-party service delivery models.

Implications

- Accept the immediate-term potential for operating in violation of existing policies and contracts until new documentation can be drafted.
- Address the invalidation of third-party risk assessments that were completed prior to the pandemic and recalibrate risk scores in light of COVID-19.
- Consider how internal and external data can be leveraged (even on an ad hoc basis) to gain visibility into third-party control environments.

Recovery and the New Reality

Prepare for subsequent virus breakouts, new government regulations, and uncertainty regarding supply chain health.

Implications

- Streamline risk assessment processes and reconsider the value of on-site reviews.
- Increase capabilities for contingent worker surveillance.
- Employ AI- and ML-driven proactive and continuous risk monitoring to mitigate further impacts to the identification, monitoring, and management of third-party risk.

Reaction and Resilience in the immediate term

Across industries, the initial COVID-19 response was a rapid reaction to continue delivering critical business services to clients and customers in the midst of urgent global healthcare and economic challenges.

This included reassuring and communicating changes to employees and swiftly managing a move from office-based work to a work-from-home model. It quickly became evident that business was not going to operate as it previously had for a long time, and that organizations were going to need to drastically change their operating models.

One aspect of the new enterprise operating model that required significant adaptation within previously unthinkably fast timelines is TPRM. To support remote work, organizations rapidly adopted third-party collaboration and video conferencing tools and fundamentally reprioritized transformation projects and third-party contracts. Organizations have turned to remote contingent workers to backfill for employees that are unable to work due to COVID-19 or to account for new, urgent priorities (particularly in financial services). For existing third parties, organizations could often no longer rely on standard, agreed-upon local security and compliance controls and have had to learn how to manage infrastructure partners and supply chains remotely.

Furthermore, third parties have long needed to revisit their own operating and service delivery models. The COVID-19 pandemic forced third parties to experiment with digital delivery of services, remote working, and split workforce. In the near-term, this required close communication between organizations and their third parties to understand how these changes affected third-party business operations (both positive and negative). Organizations may have risk accepted the potential third-party risks to allow a more agile operating environment.

TPRM implications for the Reaction and Resilience phases

These rapid, seismic shifts in the way that businesses and third parties are operating undermined the validity of the point-in-time third-party risk assessments that were completed prior to the pandemic and—more broadly—has largely paused ongoing monitoring and performance management processes.

Stakeholders across TPRM (inclusive of Procurement, Legal, Risk Management, Compliance, Cyber, and the Business) have had to modify processes to support their staff and third parties working from home.

Oftentimes, this initial shift has meant operating in violation of existing policies and contracts until new agreements can be drafted. This could include contingent workers whose contracts mandated on-site work and internal policies that require on-site reviews of critical third parties to be conducted on a regular cadence or frequency. Organizations have been challenged to reevaluate the relevancy of their definitions of third-party criticality. On-site reviews are no longer occurring—aside from limited instances of video conference walk-through exercises to test controls virtually. Internal risk management experts may have been redeployed to ensure enterprise business resilience and to support other business critical services, rather than conducting third-party risk assessment activities.

Top-of-mind concerns related to the Reaction and Resilience phases include:

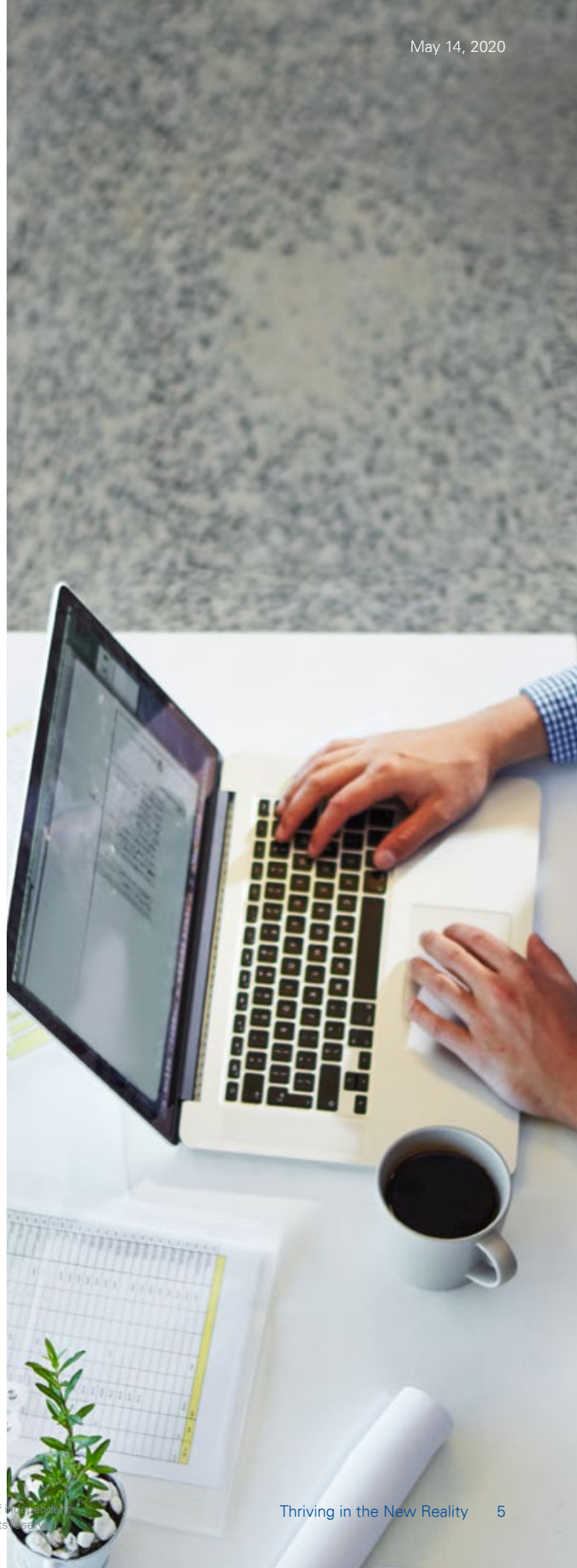
- Is my third party still meeting contractual security and operational requirements given potentially new remote operating locations? If not, how is my third-party supplementing these controls? How is the negotiation process working, and which specific terms are being prioritized over others?
- How can I gain comfort that risks are being managed if I cannot perform on-site reviews due to lockdowns? Even on an ad hoc basis, am I able to leverage internal and external data sources to gain visibility into the third party's control environment?
- Am I able to see changes in the risk posture of my entire third-party portfolio? If yes, can I timely and effectively implement a mitigation program to continue to manage the risks posed to my organization?

KPMG

- In light of COVID-19, have third parties' risk profiles increased (or decreased) due to their geographic location or the types of service(s) they are providing?
- Can my organization still demonstrate effective internal controls over financial reporting for SOX, given these concerns?
- Can I still meet my own contractual and regulatory requirements given the changes at our third parties? Am I still able to provide critical services to clients and customers of my business?
- How do I engage third parties if we cannot perform our standard onboarding procedures (e.g., fingerprinting of contingent workers)?
- Is the third party under increased financial pressure and therefore has increased financial viability risk?

These are difficult questions, given the fluidity of the situation and nature of the ongoing emergency response. In some cases, the people necessary to provide answers to these questions may not be available or may not have solutions at this point. In other cases, the supply chain impacts may take several more weeks or months to realize.

Organizations across all industries are in a similar position. Attempting to enforce pre-COVID-19 third-party expectations may not be a realistic approach. If third parties cannot respond and meet current SLAs, financial commitments, and other requirements, strict enforcement will likely not yield improved compliance and may fracture a previously good business relationship.



May 14, 2020

Recovery and the New Reality

As organizations look beyond the initial pandemic, it is possible that new infection hot zones will require sporadic lockdowns and that these might be ongoing and unpredictable.

With future implications of COVID-19 still unclear, some questions to consider for the longer-term operating model of your business include:

- Do we anticipate organizations will go back to their old practices once government lockdowns subside?
- If not, can we foresee the likely changes and proactively manage the impact to our business?
- Will organizations continue to ask employees to work from home to limit interactions in offices for an extended period (even if the government has started lifting lockdowns)?
- Will organizations continue to leverage technologies and capabilities built to support work-from-home efforts in the delivery of products and services, even after the crisis has lifted, to reduce cost?
- What will the new location strategy be?
- Will outsourcing decisions be reviewed with a view of bringing them back in house to drive resiliency or preserve full-time employee jobs?
- Similarly, will offshoring decisions be revisited to bring services back onshore and in closer proximity to your operations?
- How will the impact of global travel changes affect your ability to visit and inspect third parties across geographic locations?

KPMG

TPRM implications for Recovery

Organizations need to consider new approaches to the unknown and take time now to plan strategies to answer the following questions:

- What has changed in the third party's environment that will not go back to a pre-COVID-19 state?
- How do those changes impact third-party service delivery or increase risk?
- How can we get better visibility remotely into the critical third-party controls that impact our operations, security, and compliance as part of our business-as-usual TPRM program? What internal and external data sources can we employ?
- Did we uncover any fundamental weaknesses in a third party's control environment or ability to perform under stress that were not evident in the original point-in-time risk assessments (both remote and on-site)? Did inherent or residual risk scores prove useful in focusing efforts on the highest risk third parties, or were there surprises?
- Did business resilience plans work and how should these be adjusted?
- What considerations should be provided if these changes do not align with our current TPRM program, risk appetite, and risk management practices?
- What contractual changes need to be made to existing agreements to account for current and future pandemic response?
- What tactical changes can be made to our third-party programs to improve our ability to identify, monitor, and manage third-party risks? Will regulation and legislation evolve accordingly?

It is time to consider that all of our historical assessment information and related control environment analysis could potentially be irrelevant. Internal policies, procedures, and third-party controls all must evolve.

Recommended TPRM strategy in the New Reality

The goals of your TPRM program may now change to focus on driving better third-party performance, reducing program cost, or optimizing the efficient scalability of your assessment program.

Identify controls for continuous monitoring up front

Consider if point-in-time risk assessments and on-site reviews are still valuable

Now is the time to implement new approaches to mature your program and get the visibility you need into the ongoing performance of critical third-party controls.

Update your third-party outsourcing strategy and risk appetite in alignment with the organization's updated sourcing goals.

Re-identify which are the new critical and high-risk third parties in this operational environment. Assess concentration risk with particular emphasis on the geographic location of third parties, and consider lessons learned from third parties that were (or were not) able to consistently deliver products/services with a remote workforce.

To come back into compliance with internal policy and regulatory requirements, consider managed services, utility providers, and automated data streams in your assessment ramp-up.

Update TPRM documentation to proactively account for periods where risk assessments (particularly on-site reviews) are not viable; consider whether this is an opportunity to wholesale change risk assessment requirements.

Reevaluate how continuous controls monitoring can accomplish the goals of your TPRM program, in lieu of the standard inherent risk questionnaire, due diligence assessment, and on-site review regime.

Consider how your organization can consistently and holistically identify, monitor, and manage the third-party risks of remote contingent workers and third-party services being provided by a remote workforce, including decreased data security, increased capacity for fraud, the removal of information barriers invalidation of access controls, remote printing, and the use of personal devices for business activities.

KPMG

Determine how app-based monitoring of remote contingent workers could be incorporated into your TPRM program.

Rethink how data-driven, proactive risk monitoring, and leveraging artificial intelligence and machine learning can identify early warning indicators for third-party resilience and help mitigate the impact of future crises, including pandemics, climate-related events, and geopolitical instability.

Anticipate future disruption by scenario planning and testing. Consider further disruption to the workforce, geographical locations, changes in government policy, different restrictions that might apply, and ask for third parties to provide their own scenario plans and testing.

Update your contingency plans and exit strategies for third parties.

We are here for our clients every step of the way, as organizations continue to grapple with the uncertain challenges presented by managing third-party risk in response to COVID-19. The journey from a Reactionary state to Recovery and the New Reality is an opportunity for organizations to reconsider traditional approaches to TPRM and begin transforming their programs for the better. Reach out to learn more about KPMG's TPRM service offerings and how we can work together to thrive in the New Reality.

Contact us

KPMG has been investing heavily in driving process excellence, third-party automation, threat intelligence, and managed services.

Please contact us to learn more about ways we can assist your program to thrive in the New Reality.

U.S. contacts

Jonathan Dambrot
Principal, Advisory
KPMG in the U.S.
E: jdambrot@kpmg.com

Greg Matthews
Partner, Advisory
KPMG in the U.S.
E: gmatthews1@kpmg.com

Tarun Sondhi
Principal, Advisory
KPMG in the U.S.
E: tsondhi@kpmg.com

Amanda Rigby
Principal, Advisory
KPMG in the U.S.
E: amandarigby@kpmg.com

Global contacts

Jon Dowie
United Kingdom
E: jon.dowie@kpmg.co.uk

Alexander Geschonneck
Germany
E: ageschonneck@kpmg.com

Gavin Rosettenstein
Australia
E: gavin1@kpmg.com.au

Contributors

Michael Falk

Natalie Fedyuk

Sarah Gross

Rangana Guha

Nicole Lauer

Priya Mouli

Thomas Nash

Sebastian Pronk

Anne Schmitt

Nicole Trawick

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia