KPMG

R.G. Manabat & Co.

Transitioning to a new normal

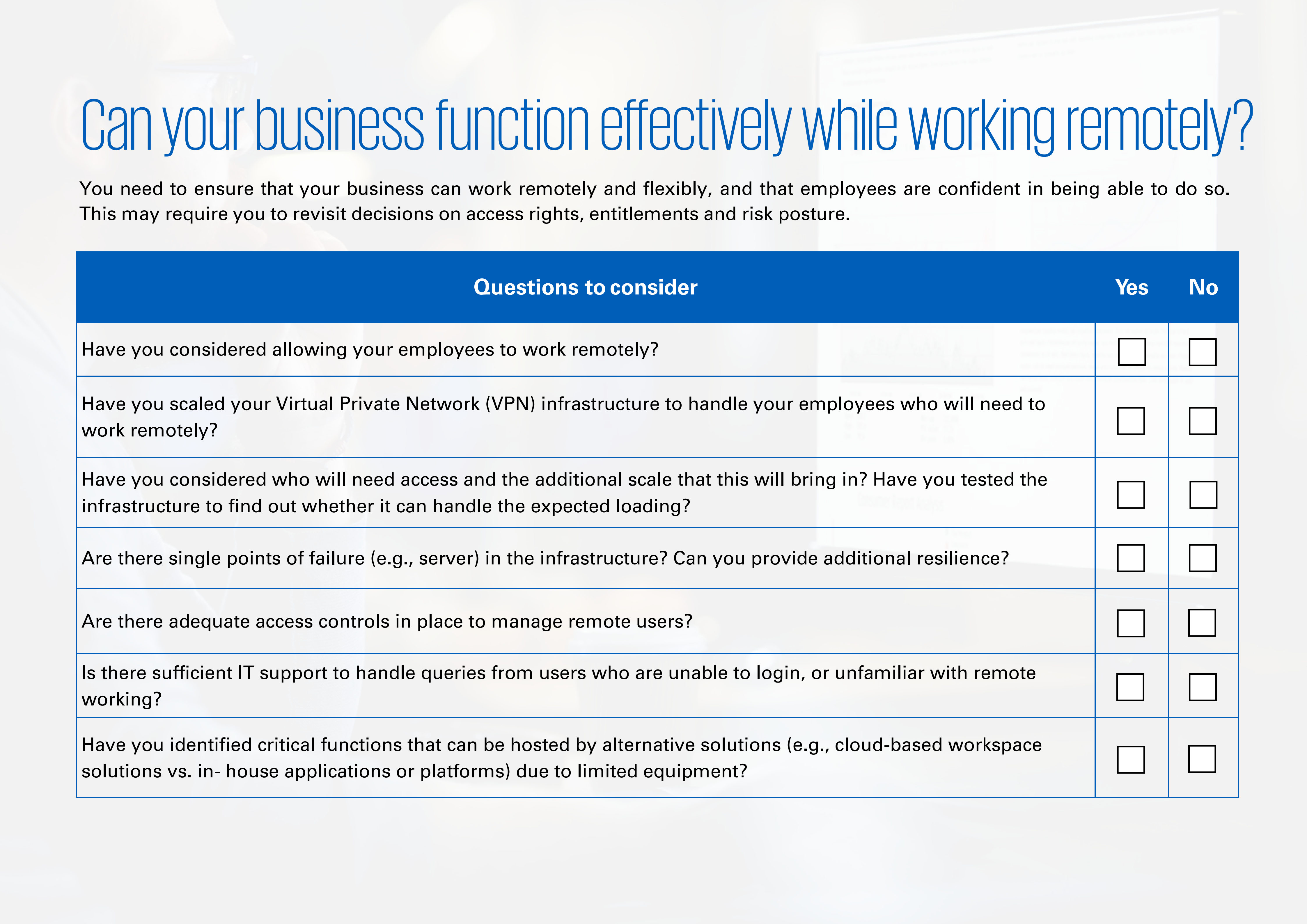
Maintaining digital resilience post-pandemic

April 2020

Is your business digitally resilient?

With the evolving COVID-19 pandemic, organizations need to rethink strategies to drive resilience and sustain business. As a leader, you must optimize all business functions as containment measures are being implemented.

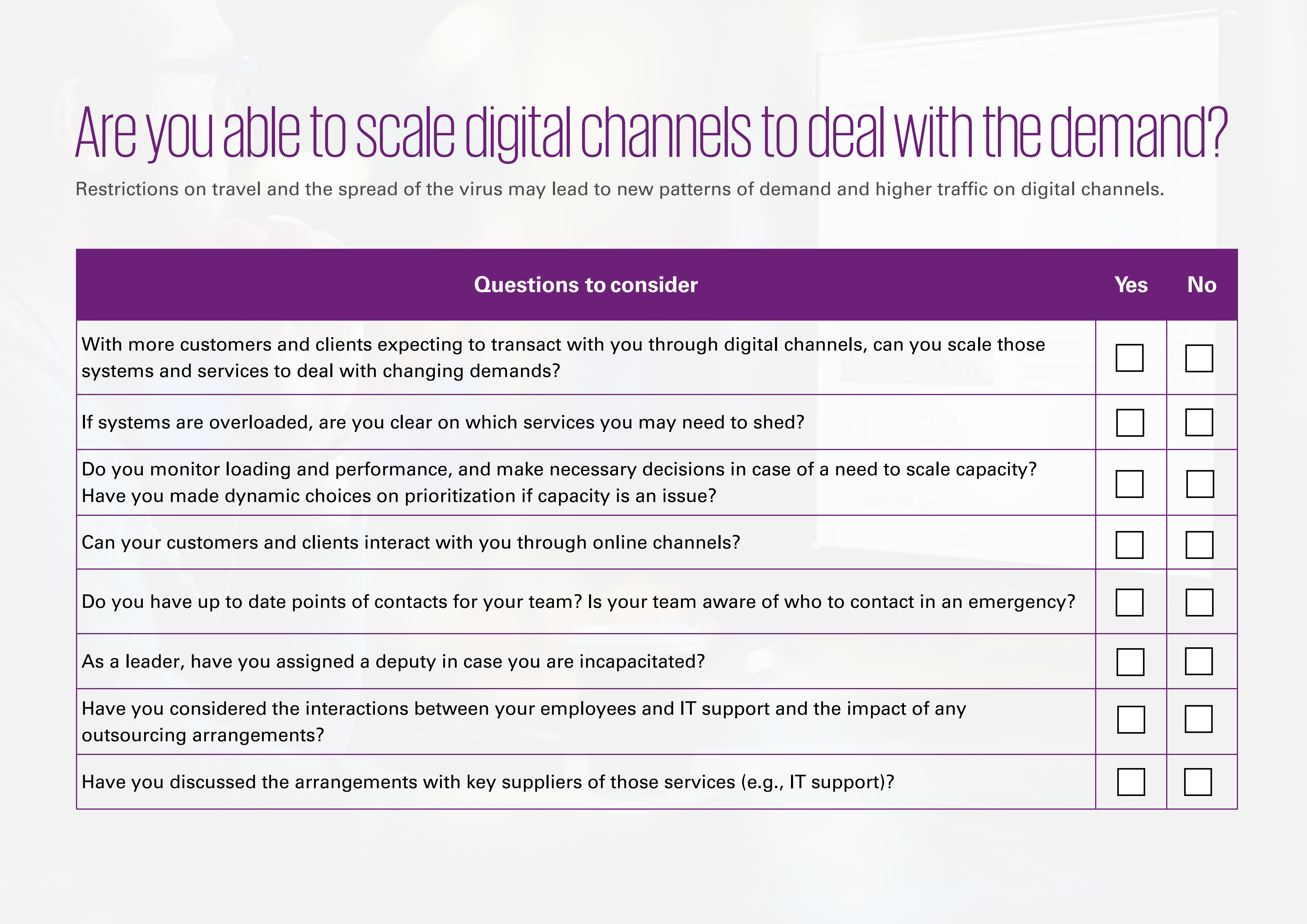
To help you navigate through this crisis, we have prepared key questions and five security domains to consider during and after the pandemic.



Can your business function effectively while working remotely?

You need to ensure that your business can work remotely and flexibly, and that employees are confident in being able to do so. This may require you to revisit decisions on access rights, entitlements and risk posture.

Questions to consider	Yes	No
Have you considered allowing your employees to work remotely?	□	□
Have you scaled your Virtual Private Network (VPN) infrastructure to handle your employees who will need to work remotely?	□	□
Have you considered who will need access and the additional scale that this will bring in? Have you tested the infrastructure to find out whether it can handle the expected loading?	□	□
Are there single points of failure (e.g., server) in the infrastructure? Can you provide additional resilience?	□	□
Are there adequate access controls in place to manage remote users?	□	□
Is there sufficient IT support to handle queries from users who are unable to login, or unfamiliar with remote working?	□	□
Have you identified critical functions that can be hosted by alternative solutions (e.g., cloud-based workspace solutions vs. in- house applications or platforms) due to limited equipment?	□	□



Are you able to scale digital channels to deal with the demand?

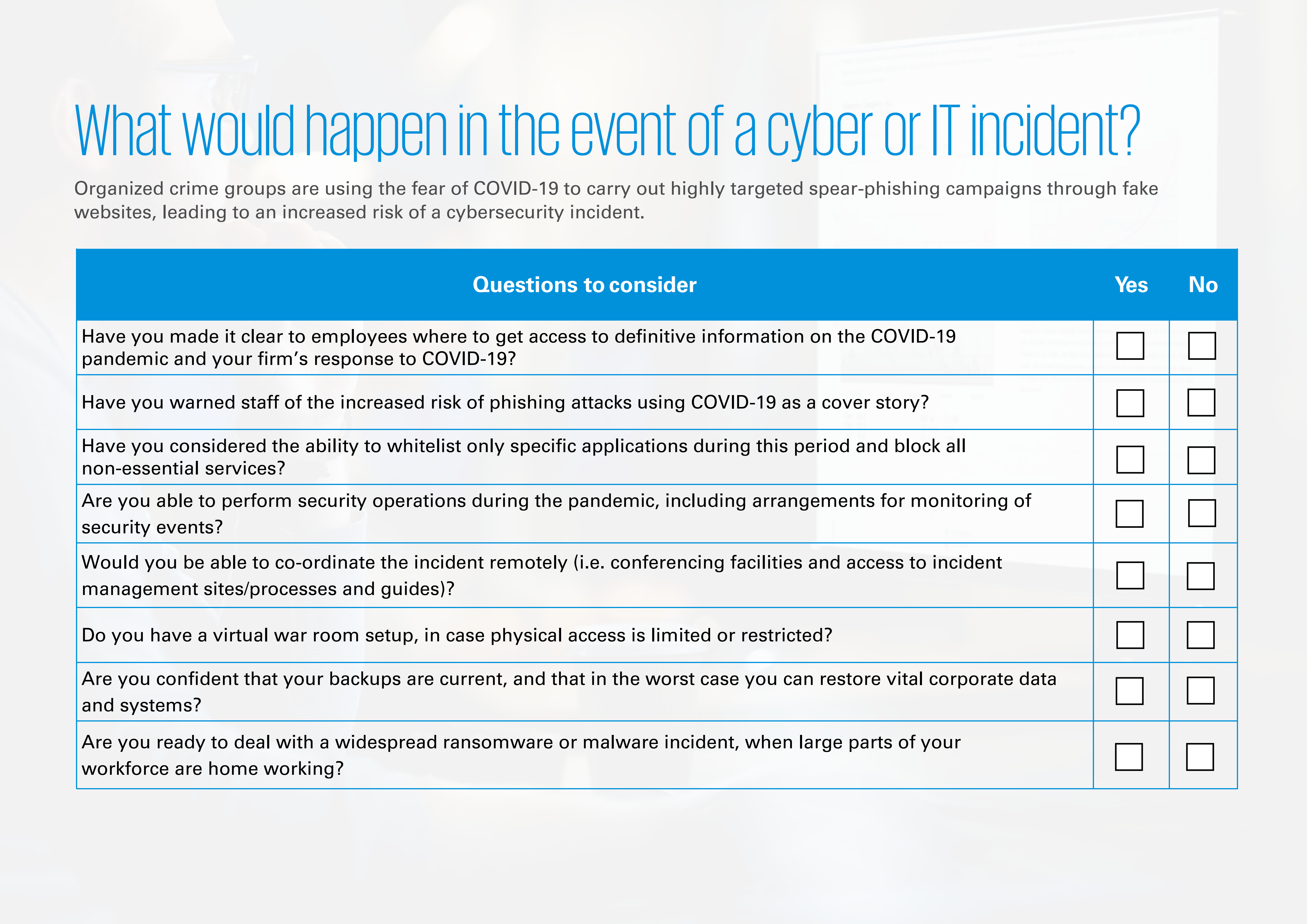
Restrictions on travel and the spread of the virus may lead to new patterns of demand and higher traffic on digital channels.

Questions to consider	Yes	No
With more customers and clients expecting to transact with you through digital channels, can you scale those systems and services to deal with changing demands?	□	□
If systems are overloaded, are you clear on which services you may need to shed?	□	□
Do you monitor loading and performance, and make necessary decisions in case of a need to scale capacity? Have you made dynamic choices on prioritization if capacity is an issue?	□	□
Can your customers and clients interact with you through online channels?	□	□
Do you have up to date points of contacts for your team? Is your team aware of who to contact in an emergency?	□	□
As a leader, have you assigned a deputy in case you are incapacitated?	□	□
Have you considered the interactions between your employees and IT support and the impact of any outsourcing arrangements?	□	□
Have you discussed the arrangements with key suppliers of those services (e.g., IT support)?	□	□

What would happen if data center disruption occurs?

A confirmed COVID-19 case may result in an evacuation and deep cleaning of the building; transport infrastructure disruption may prevent access and data center staff may be unable to work.

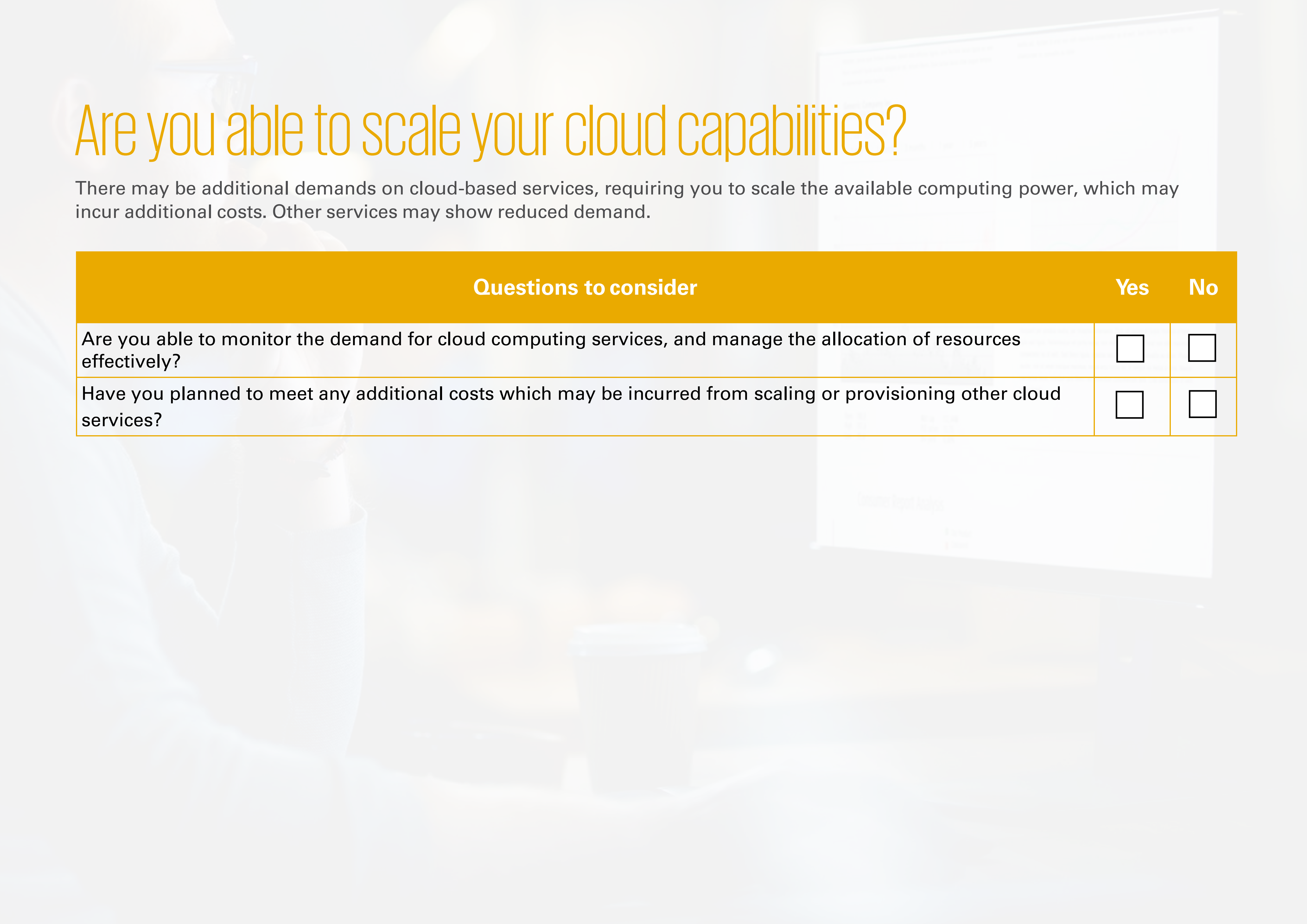
Questions to consider	Yes	No
Should one of your data centers need to be evacuated, do you have disaster recovery plans in place to deal with the disruption?	□	□
Do you have a quick failover plan to go to an alternate site?	□	□
Are you dependent on external contractors for the operation of the data center?	□	□
If you are dependent on external contractors, do you have an alternative plan to manage that dependency?	□	□
Are there steps you could take to reduce external contractor dependency, including using your team resources?	□	□
Are you discussing the implications with your key suppliers, and do you have the right points of contact with those suppliers?	□	□
Have you identified which IT suppliers may come under financial pressure, and what would be your alternate sourcing strategy should they fail?	□	□



What would happen in the event of a cyber or IT incident?

Organized crime groups are using the fear of COVID-19 to carry out highly targeted spear-phishing campaigns through fake websites, leading to an increased risk of a cybersecurity incident.

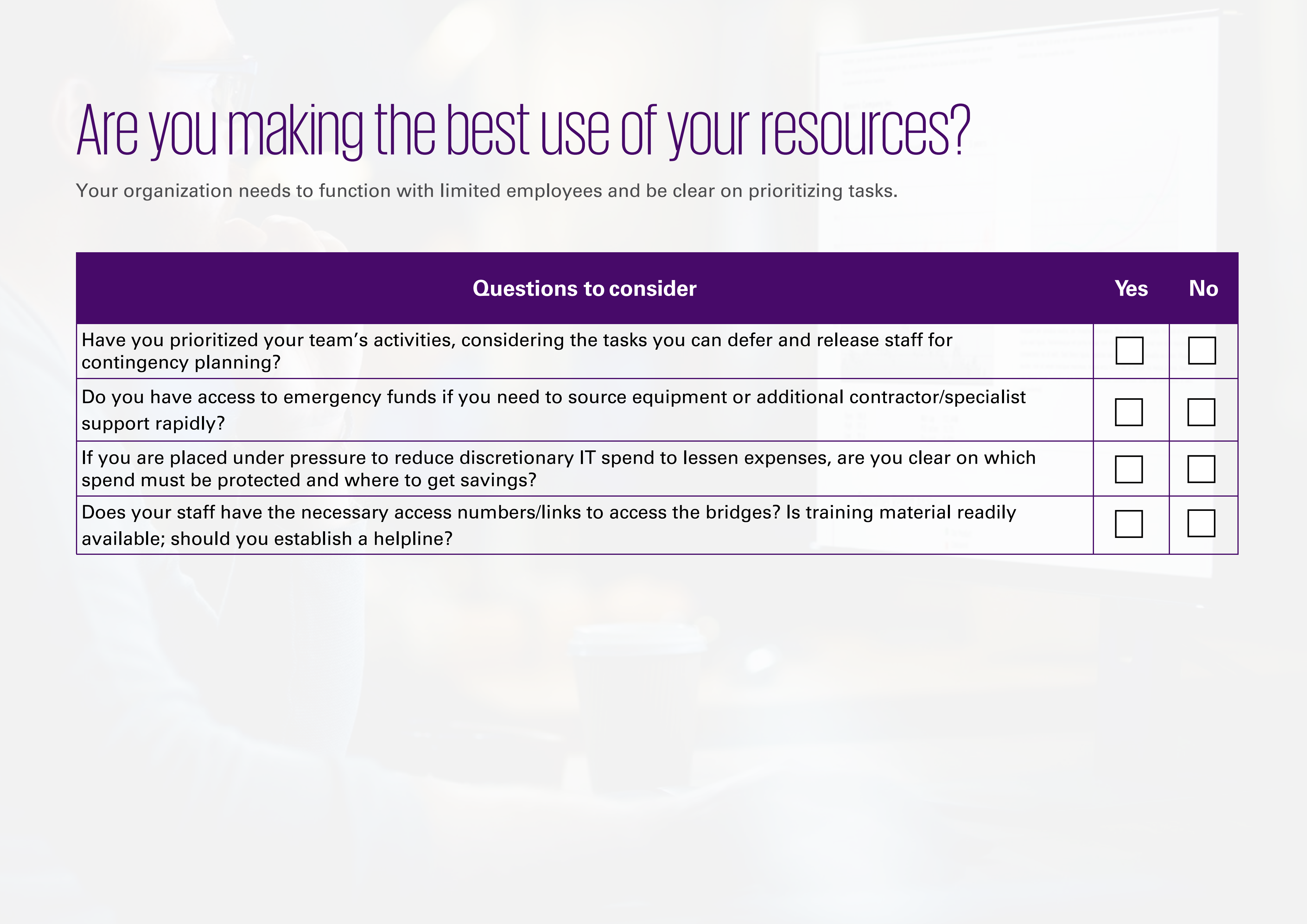
Questions to consider	Yes	No
Have you made it clear to employees where to get access to definitive information on the COVID-19 pandemic and your firm’s response to COVID-19?	□	□
Have you warned staff of the increased risk of phishing attacks using COVID-19 as a cover story?	□	□
Have you considered the ability to whitelist only specific applications during this period and block all non-essential services?	□	□
Are you able to perform security operations during the pandemic, including arrangements for monitoring of security events?	□	□
Would you be able to co-ordinate the incident remotely (i.e. conferencing facilities and access to incident management sites/processes and guides)?	□	□
Do you have a virtual war room setup, in case physical access is limited or restricted?	□	□
Are you confident that your backups are current, and that in the worst case you can restore vital corporate data and systems?	□	□
Are you ready to deal with a widespread ransomware or malware incident, when large parts of your workforce are home working?	□	□



Are you able to scale your cloud capabilities?

There may be additional demands on cloud-based services, requiring you to scale the available computing power, which may incur additional costs. Other services may show reduced demand.

Questions to consider	Yes	No
Are you able to monitor the demand for cloud computing services, and manage the allocation of resources effectively?	□	□
Have you planned to meet any additional costs which may be incurred from scaling or provisioning other cloud services?	□	□



Are you making the best use of your resources?

Your organization needs to function with limited employees and be clear on prioritizing tasks.

Questions to consider	Yes	No
Have you prioritized your team’s activities, considering the tasks you can defer and release staff for contingency planning?	□	□
Do you have access to emergency funds if you need to source equipment or additional contractor/specialist support rapidly?	□	□
If you are placed under pressure to reduce discretionary IT spend to lessen expenses, are you clear on which spend must be protected and where to get savings?	□	□
Does your staff have the necessary access numbers/links to access the bridges? Is training material readily available; should you establish a helpline?	□	□

If most of your answers from the previous questionnaire are “No,” you need to reassess your digital resilience and readiness to support and sustain your business.

Now is the time to get your functional domains of cyber operations in place.

Incident Command and Control must be maintained under remote work conditions

- ✓ Ensure relevant communications plan (e.g., employees should be aware of how to contact security)
- ✓ Ensure ransomware playbook awareness and revision (e.g., consider working from home scenarios)
- ✓ Integrate cyber into crisis management. (e.g., privacy, public affairs)
- ✓ Focused defensive planning for threats brought on by the pandemic
- ✓ Better integrate with the industry through ISACs

Command

Capabilities to enable decision making and oversee security operations.

Security monitoring must adapt and persevere

- ✓ Ensure all security controls are updated and logging is enabled properly
- ✓ Ensure remote forensics capability (e.g., remote image collection)
- ✓ Review use cases for effectiveness as the network behavior has changed
- ✓ Ensure actioning of any lost network visibility due to working from home (e.g., use IDS/IPS)
- ✓ Enhance User and Entity Behavior Analytics (UEBA) monitoring to enhance insider threat and anomaly monitoring
- ✓ Review technology portfolios with incumbent vendors to easily add Features instead of new procurement cycles
- ✓ Increase insider threat monitoring due to higher global employment uncertainty

Sense

Ability to detect cyber events of interest. (e.g., Security Controls and SIEM)

Response capabilities extend to remote working conditions

- ✓ Ensure vendor contact information and that SLAs are reviewed and understood by security personnel
- ✓ Review emergency change management processes to expedite approvals
- ✓ Ensure user termination processes are functioning end to end (e.g., all access drops upon user termination)
- ✓ Ensure all administrative actions are logged
- ✓ Employ Security Orchestration and Response Automation (SOAR) methodologies
- ✓ Employ Network Access Controls (NAC) through existing technologies or manual processes such as MAC whitelisting

Act

Ability to contain and remediate an incident once it is discovered

Cyber risks introduced due to remote working conditions and persistent threat actors will continue to evolve

- ✓ Conduct blue team review of email and VPN access control postures
- ✓ Ensure full review of identity and access management and authentication posture
- ✓ Monitor the perimeter for unintended network exposures
- ✓ Communicate guidelines for employees to secure their home networks
- ✓ Ensure all security technologies are being updated as needed
- ✓ Ensure sensitive/ VIP positions have additional over-watch especially in home networks
- ✓ Carry out purple teaming activities to validate that network is secure against known attack patterns

Shield

Reactive and proactive hardening of the organization. (e.g., vulnerability management)

The Cyber Operations function now extends to an expanded threat surface

- ✓ Security teams must prepare to operate remotely, but potentially within company infrastructure if cut off from the network
- ✓ Ensure security responders have a secure location and infrastructure where they can respond effectively to cyber events.
- ✓ Strictly forbid the use of unmanaged personal devices for work duties (e.g., home PC)
- ✓ Review Cyber-Insurance coverage given remote work posture and changing attack surfaces
- ✓ Secure E-supply chain (e.g., container libraries, imported code, vendor widgets)
- ✓ Establish redundant vendor pipeline for critical IT capabilities (e.g., firewall)

Sustain

Ability to sustain your cyber posture over the short and long run

R.G. Manabat & Co.

Consult with us:

Jallain Marcel S. Manrique

Partner and Head of Digital and IT Advisory
+63 917 621 4052
jsmanrique@kpmg.com

Michael Glenn B. Kakumoto

Director, Cyber Security
+63 917 572 4237
mbkakumoto@kpmg.com

Gilbert T. Trinchera

Senior Manager, Digital and IT Advisory
+63 917 569 4000
gttrinchera@kpmg.com

Know more about our services: