KPMG

Contextualising third party onsite assessment in COVID-19 era

October 2020

home.kpmg/in

Introduction

Third Party Risk Management (TPRM) has become a key risk management discipline and has attracted significant attention from the regulators, boards, leadership, customers and other key stakeholders. Third party onsite assessment has been a core component of TPRM framework across organisations. Onsite assessments help the organisations to:

- Comply with regulatory requirements
- Perform a sense check and understand third party organisation risk culture
- Measure third party staff awareness of key requirements
- Get deeper and focused risk insights related to specific areas.

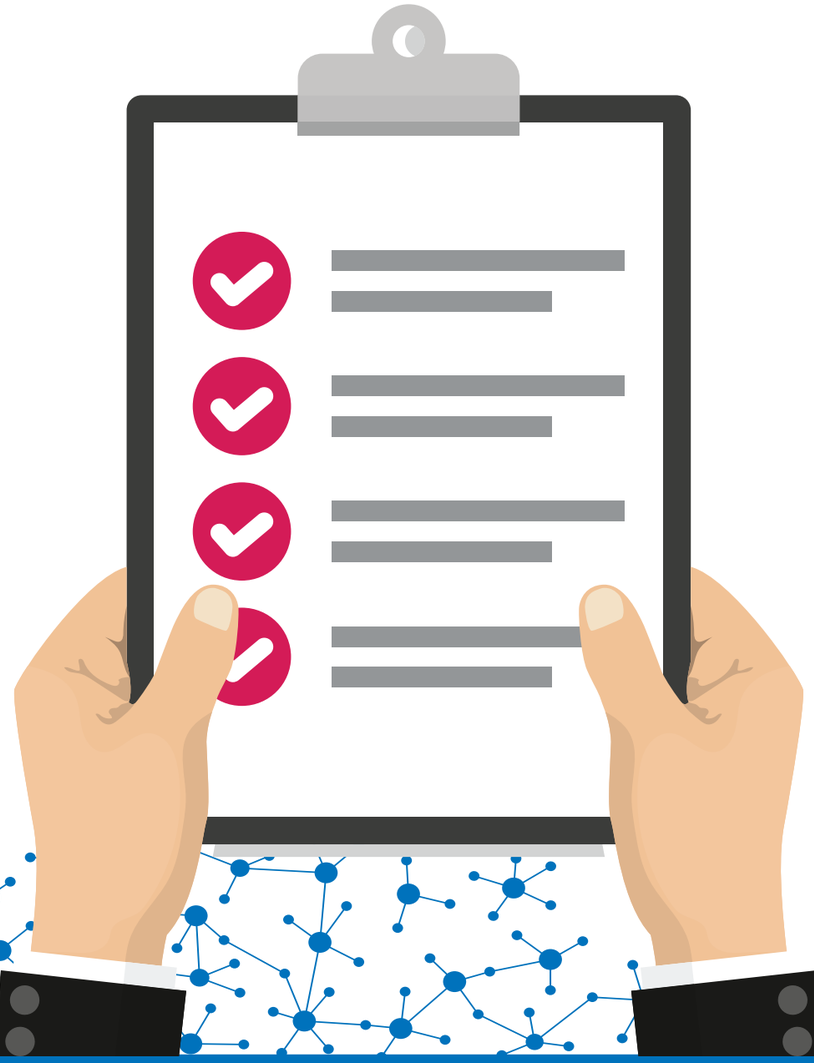
Further, onsite assessments follow ‘trust but verify’ approach, in terms of physical walkthrough and observation for areas requiring greater assurance.

However, the COVID-19 pandemic has brought unprecedented disruptions across multiple sectors impacting the business activities of organisations and their third parties. The COVID-19 pandemic not only amplified the impact of third party and supply chain disruption but also challenged ability of global organisations to plan and execute key third party risk management components such as onsite assessments.

This point of view document outlines specific considerations in the wake of COVID-19, which organisations may consider while defining an alternative to existing approach for onsite assessments.

Key challenges in conducting third party onsite assessment during COVID-19

- How do you plan to meet regulatory requirements or business function's request for a third party onsite assessment?
- Have you updated your third party risk management framework to include the following?
  - To provide risk acceptance/risk exemption resulting from third party onsite assessments not being performed
  - To revisit the risk segmentation criteria and triggers to determine which third parties and third party contractual arrangements should qualify for an onsite assessment
  - To maintain continuous oversight on the risk posture of third parties and risk exposure to organisation due to third parties
  - Risk domains that require heightened ongoing monitoring.



Measures to address challenges in conducting third party onsite assessment during COVID-19

In the wake of COVID-19 pandemic, global organisations are in discussions with regulators, boards, committees, the second line of defense (LoD2) and the third line of defense (LoD3) stakeholders and are refreshing their onsite assessment strategy to address the restrictions and challenges.

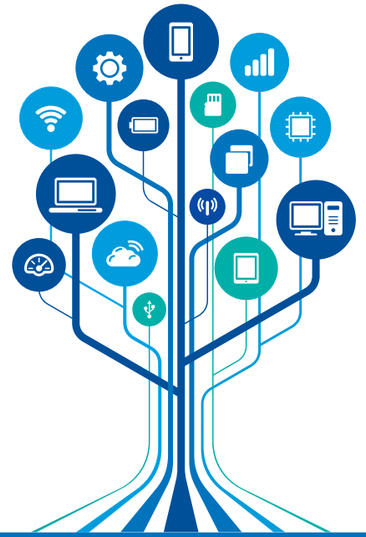
Key levers considered as part of this strategy refresh include but not limited to:

1. Risk acceptance by an appropriate authority
2. Deferment of onsite assessments
3. Leverage external risk intelligence to perform focused assessments
4. Continuous assurance and monitoring (CAM)
5. Reliance on assurance reports such as ISAE 3000, SOC 1 Type 1/2, SOC 2 Type 1/2, PCI-DSS
6. Reliance on audit report/ other independent reports (performed by independent team/ LoD 2/ LoD3)
7. Self-assessment review
8. Online assessments for evaluating controls remotely
    - Online tour of third party facility
    - Review of compensating control evidence
    - Sharing of system configuration screenshots or other evidence through various collaboration platforms.

Most organisations have leveraged a combination of levers, however, online assessments have emerged as an important mechanism in lieu of onsite assessments until there is a potential opportunity to conduct physical onsite assessments. Key aspects related to online assessments are outlined below:

1. Comparison between remote assessment and online assessment

Parameters	Remote assessment	Online assessment
Degree of interaction	Low degree of interaction between the assessor and third party, primarily through e-mail	High degree of interaction between the assessor and third party leveraging multiple communication channels
Document review	Third parties prefer not to share evidence documentation, especially when they contain confidential information, for remote review	Evidence documentation containing highly confidential information can be accessed and reviewed with use of collaborative platforms and data sharing platforms (Virtual Data Rooms (VDR), Managed File Transfer (MFT), Secure File Transfer Protocol (SFTP)
Control coverage	Operating effectiveness of the following control areas can't be assessed: Physical security System security requiring configuration review	Operating effectiveness of the following control areas can be assessed: Physical security – Augmented Reality (AR)/Virtual Reality (VR) technology can be leveraged to perform 360-degree video-graphic view of the facility System security requiring configuration review- Collaborative and data sharing platforms as highlighted above can be used
Environment	Offline review	Technology enables assessors to create an environment similar to an onsite assessment



2. Online assessment process flow

Notification to the third party about the objective of the assessment and the initiation call date and time

Initiation call with third party to discuss and outline specifics of collaboration platforms to be leveraged during the course of the assessment

Share day-wise assessment agenda for meetings, sharing of data, facility tour etc.

Conduct interview with third party stakeholders leveraging agreed collaboration platform to obtain process walkthrough and review documents and supporting evidence for select controls. For highly confidential documents, leverage data sharing platforms

Discuss observations with third party and agree on root cause, action plan and remediation date

Release the report

3. Assessing traditional onsite assessment areas through online assessment

Outlined below are traditional onsite assessment control areas that can be assessed through alternate approaches leveraging collaboration platforms, data sharing platforms and AR/VR.

Control area	Traditional onsite assessment	Online assessment
Policy review	Review of policies that can't be shared for remote review	**Technology:** Collaboration platforms and video conferencing allows third parties to share documents and actively participate in the assessment **Effectiveness:** High
System configuration	• Process walkthrough • For select systems, verification of system configuration	**Technology:** Collaboration platforms and video conferencing allow third parties to share documents and actively participate in the assessment **Effectiveness:** High
Highly confidential information	Review of staff vetting reports, insurance documents, invoices, documents that contain employee or client identifying data and can't be shared for remote review	**Technology:** Data sharing platforms - VDR, MFT, SFTP, Intralinks allow third parties to share confidential documents and supporting evidences. These documents can be removed/deleted from the SFTP links by the third party once the assessment is completed **Effectiveness:** High
Physical security	1. Process walkthrough 2. Site walkthrough	**Technology:** AR/VR technology can provide a 360-degree video graphic view of the site **Effectiveness:** Medium; AR/VR has its own limitations like data privacy concerns, accessibility to third party premise during lockdown and required set of skills to operate AR/VR tools

4. Potential scenarios where online assessment may not work effectively

Mandatory requirement to conduct third party onsite visit to close regulatory or business findings

Third party does not have remote access to the servers, end-point devices, infrastructure components (switch, routers, firewalls, etc.) and applications

Data privacy concerns, accessibility to third party premise during lockdown and required set of skills to operate. Third party has data confidentiality concerns in remote sharing of evidences

Third party providing services from an 'air gapped' offshore development center without access to internet

Case study

Background

A global bank was required to perform third party onsite assessments to meet regulatory expectations and organisation mandate. Bank was required to design an onsite assessment framework and execute third party assessments. However, due to the ongoing COVID-19 pandemic, onsite visit to third party site was not feasible and therefore transformed the onsite assessment framework to an online assessment framework, with our assistance.

Approach

Designed and finalised the following approach with appropriate risk committee, second line and third line of defense and other key stakeholders:

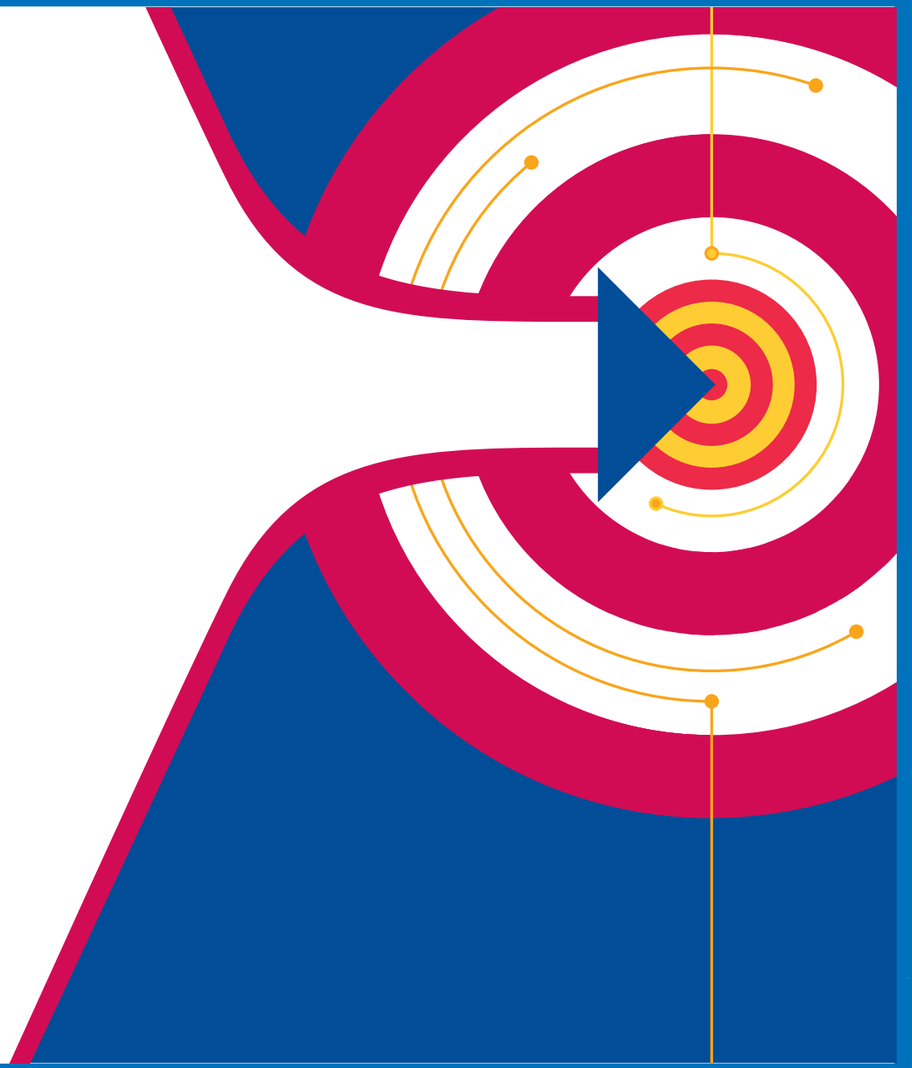
- Reliance on assurance reports such as ISAE 3000, SOC 1 Type 1/2, SOC 2 Type 1/2, PCI-DSS, etc. covering the assessment period. Additionally, self-affirmation from the third party that there has been no change in the control environment
- Virtual tour of the third party facility via web camera, etc.
- Sharing of system configuration screenshots through collaboration platforms
- Reliance on compensating control evidences for select control areas.

Outcome

Completion of third party assessments, as agreed with concerned stakeholders. Further, insights into the risk exposure, types of issues per third party type.

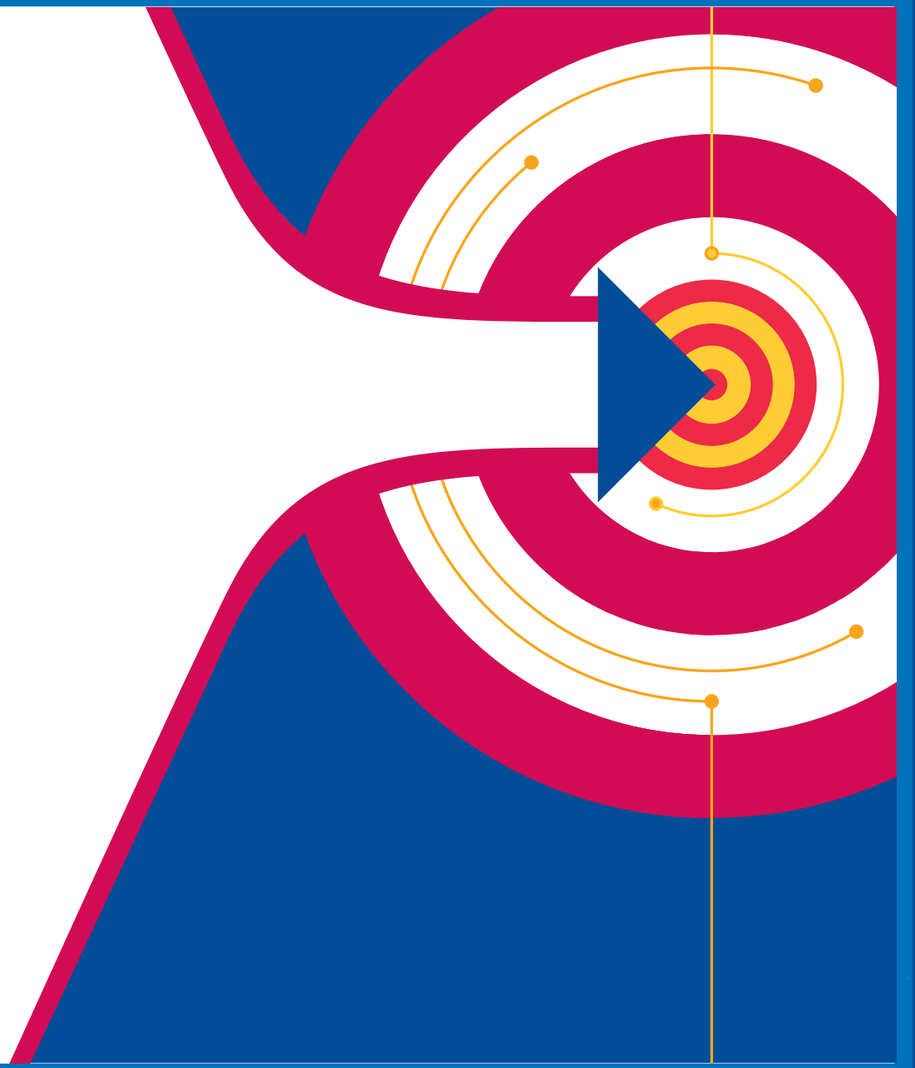
Conclusion

- The COVID-19 pandemic may have triggered a long-term change in the way organisations conduct onsite assessments
- It is essential that organisations adapt to the evolving environment and equip themselves for more effective and efficient ways of performing onsite assessments
- Online assessment methodology will mature over a period of time as both the assessors and the third party get used to the new way of performing assessments
- Onsite assessment cannot be fully replaced by online assessment, however, in this point of view document, we have outlined specific considerations in the wake of COVID-19, which organisations may consider while defining an alternative to the existing approach for onsite assessments



Acknowledgements

Srikant Rao
Abhishek Bele
Umang Saini
Nisha Fernandes
Darshini Shah
Shruti Iyer



KPMG in India contacts

Srinivas Potharaju
Partner
IT Advisory
Risk Transformation Leader
T: +91 984 591740
E: srinivasbp@kpmg.com

Srijit Menon
Director
Risk Transformation
Third Party Risk Management Leader
T: +91 973 177 7099
E: srijitmenon@kpmg.com

Rohan Padhi
Executive Director
IT Advisory
Risk Transformation
T: + 91 9930224081
E: rohanpadhi@kpmg.com

Romharsh Razdan
Director
IT Advisory
Risk Transformation
T: + 91 9975596366
E: romharsh@kpmg.com

Nitin Shah
Partner
IT Advisory
Cyber Security
T: +91 9560244888
E: nitinshah@kpmg.com

Vartika Saxena
Director
IT Advisory
Audit and Assurance
T: +91 9000921114
E: vartikasaxena@kpmg.com

Sabarinath NM
Director
IT Advisory
Audit and Assurance
T: +91 9790964344
E: sabarinathnm@kpmg.com

home.kpmg/in

#KPMG josh

Follow us on:
home.kpmg/in/socialmedia

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.