‘Offshore Development Centre’ to ‘remote working’ - addressing elevated third party risk

February 2022

home.kpmg/in

Introduction

With evolving business needs, global organisations continue to partner with third parties in performing their operations effectively and efficiently. Third Party Risk Management (TPRM) programme within these organisations also have expanded, to assess the risks arising from third party relationship types and make informed risk decisions. There are three major factors that have come into play with the outbreak of COVID-19 leading to multiplication of third party risks:

Increased digitisation and cloud adoption by the organisations increasing the number of third party relationships

Changes in existing third party's service delivery model and ways of working

Increased regulatory scrutiny to understand organisation's response to aforementioned factors.

Third parties setting up Offshore Development Centres (ODC)/Offshore Work Centres (OWC) to service global organisations/clients has been a key aspect of Information Technology Outsourcing (ITO)/Business Process Outsourcing (BPO)/Legal Process Outsourcing (LPO) industry. Such ODCs/OWCs provide a controlled third party environment with stringent physical and logical security controls. However, the COVID-19 pandemic has disrupted this well-established service delivery model and pushed third parties to adopt a 'remote setup' model in the short term and hybrid setup represented by mix of ODC/OWC and remote setup in the long term. This change in service delivery model has challenged organisation's existing understanding of its third party risk exposure. In this point of view, we at KPMG in India have highlighted key aspects of elevated third party risk exposure resulting from this change and suggested practical considerations for organisations to assess and manage the risks.

Key changes leading to heightened third party risk profile

Key factors contributing to increased risks as a result of remote/hybrid setup include:

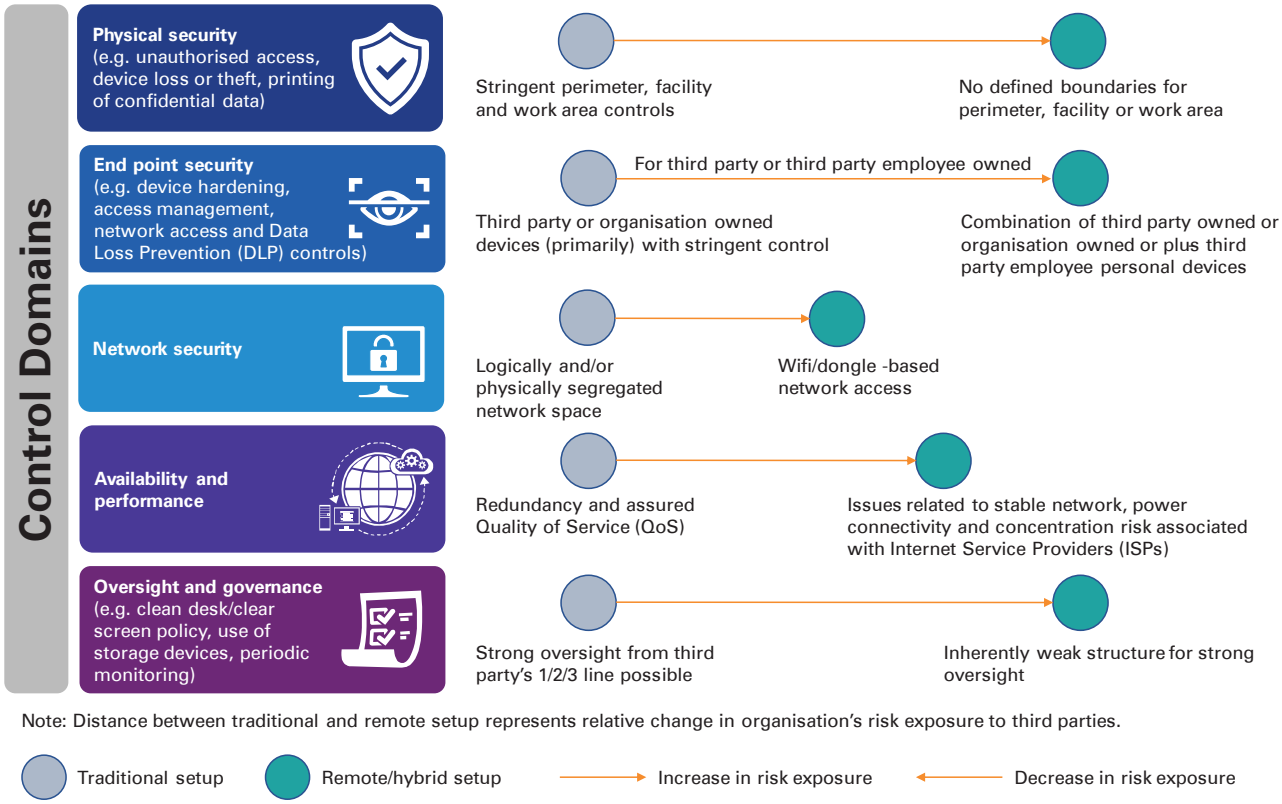
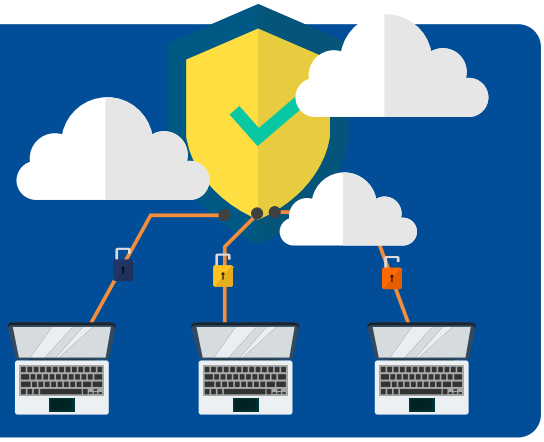
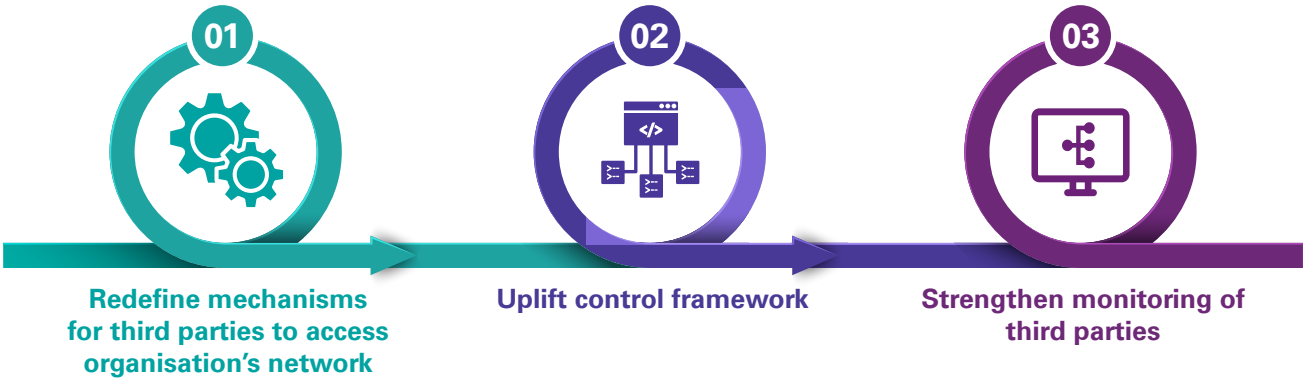


Image 1: Key factors contributing to heightened risks

Considerations that organisations and third parties are evaluating to contain risk exposure



Organisations are using a combination of below mentioned measures to address elevated third party risk environment:



1. **Redefine mechanisms for third parties to access organisation's network:**

   Organisations are selecting between four modes of granting access to its network and three ownership models for endpoint devices used by third parties. The selected combination of these two factors determines inherent technology risk exposure to organisations (thereby driving decision on technology controls to be implemented by third parties and monitored by organisations) and associated cost implications.

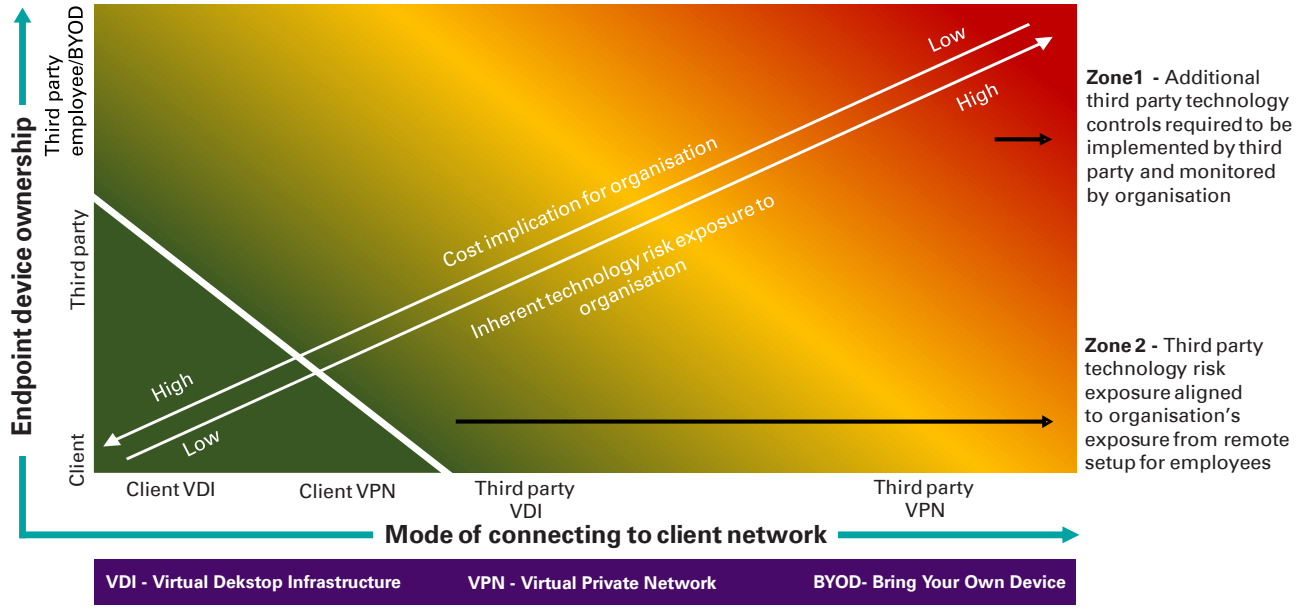


Image 2: Impact on risk profile due to different modes of connecting to client network

Note: Some of the combinations (such as third party Virtual Desktop Infrastructure (VDI) on client owned device or third party Virtual Private Network (VPN) on client owned device) represented in the graph above, are generally not observed in practice.

2. Uplift control framework:

Organisations are enhancing their third party control framework to address risks from remote/hybrid setup. List of illustrative controls implemented are mentioned in the table below. These controls may vary depending on type of services provided by the third party, mode of connecting to client network and endpoint device administration and ownership.

Controls domains	Key considerations
1 Physical security	a. Concept of work area in remote working setup b. Secure work area controls such as clean desk, clear screen, use of privacy filters/screen protectors c. Secure transit/handling of assets (including laptop/workstation/ dongle etc. movement from office premise to employee locations, maintenance and repair of these assets).
2 Network security	a. Secure configuration for VDI infrastructure b. Secure configuration for VPN infrastructure (e.g. split-tunneling disabled etc.) c. Secure configuration of home internet connection d. Secure third party network configuration for Bring Your Own Device (BYOD)/third party devices e. White-listing of the Internet Protocol (IP) address(es) connecting to third party's network.
3 Endpoint security	a. Mobile Device Management (MDM) solution for enrollment, device management, software deployment, machine policy management and disablement b. Anti-virus deployment for virus and malware detection c. Security patch deployment and update d. Data Leakage Protection (DLP) controls e. BYOD asset management policy f. Access to public sites disabled on devices via web filtering tools g. Network (if applicable) and end point device encryption to secure data at rest and transit.
4 Availability and performance	a. Last mile network reliability b. Concentration risk associated with internet service providers c. Third party pandemic response plan.
5 Oversight and governance	a. Virtual onboarding (including interview, recruitment, and background verification processes) and offboarding of employees (secure handover of assets, access cards, data deletion etc.) b. Declarations from third party employees in context of secure ways of remote working c. Information security awareness training programmes to re-emphasise on threats relevant to remote working scenario d. Review of remote access VPN connections to organisation's network e. Spot online audits for clean desk controls at employee's Work From Home (WFH) environment f. Monitoring of employee productivity g. Uplifted control framework for SOC1/SOC2/Agreed-Upon Procedures (AUP) audits.

Table 1: Uplifted control domains and key considerations

3. Strengthen monitoring of third parties:

Measures that are being considered by organisations to strengthen their monitoring mechanism include:

a

Implement cyber threat intelligence solutions to monitor traffic originated from third party devices/network on a real time basis.

b

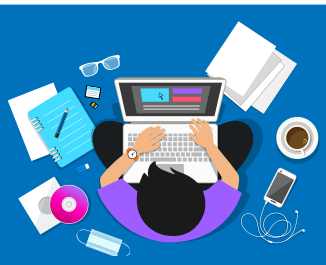
For all the devices connecting to organisation's network or accessing data, maintain oversight on:

- personnel who are accessing the device
- location from where the device is connected
- mode of connecting to organisation's infrastructure
- compliance posture of endpoint devices.

c

Establish process to monitor effective implementation of controls which has been put in place by the third party to address risks associated with all five control domains (physical security, network security, endpoint security, network availability and performance, oversight and governance) as mentioned in 'Table 1- uplifted control domains and key considerations.'

Case study



Organisations across sectors have responded in different ways to the elevated third party risks resulting from remote working. One such case study is included below:

Background:

The client is a multinational conglomerate headquartered in the United States and has outsourced its business processes with access to customer data (as relevant) to third parties. In line with the organisation's policy requirements, client is required to conduct assessment of its third parties.

Problem statement:

Prior to onset of pandemic, the third parties were working from an ODC setup for delivering services. With the shift to remote working model, client was exposed to elevated third party risks and wanted to strengthen the control environment to evaluate specific risks.

Approach:

To address some of these challenges due to change in service delivery model, client took below measures:

1. Define remote connectivity mechanism:
   Third party employees connect to client's infrastructure via client VPN from third party/client owned endpoint devices. Client VPN is configured for multi-factor authentication (credential + soft token/hard token). For third party staff dedicated to providing services to the client, BYOD is prohibited.
2. Uplift control framework:
   Organisation introduced new set of controls focused on 'remote access and business resilience' to assess its third party's preparedness with respect to WFH model.
3. Accept risk:
   Organisation provided exception approval to third parties for cases where third party was unable to meet the obligation due to constraints posed by remote working (e.g. return of assets as on 'last working day' of employee).

Conclusion

With 'future of work' moving towards a remote/ hybrid working model from the traditional ODC/ OWC setup, it is essential for organisations to reevaluate their existing strategy for addressing risks associated with such third parties.

Each global organisation is required to adopt different types of remote working model (based on selected combination of type of network access and type of endpoint access) based on the risk exposure from a third party and cost involved in enabling a particular remote working model. Key points to consider when deciding on a third party remote setup include the following – type of service provided by third party, type of data accessed, criticality of operations, maturity of third party risk monitoring programmes and organisation's risk appetite.

Further, uplifting control library as highlighted above and implementation of automated means of monitoring third party accesses will help organisation to strengthen monitoring of third party controls and take proactive measures in case of potential threats.

KPMG in India contacts:

Srinivas Potharaju
Partner,
National Co-Head - Digital Risk, Security and Governance (DRSG),
Global Capability Centre (GCC) Leader for Digital
P: +91 9845919740
E: srinivasbp@kpmg.com

Rohan Padhi
Partner,
Digital Trust
P: +91 99302 24081
E: rohanpadhi@kpmg.com

Mayuran Palanisamy
Partner,
Digital Trust
P: +91 96000 57046
E: mpalanisamy@kpmg.com

Srijit Menon
Director,
Digital Trust
National Third Party Risk Management Leader
P: +91 97317 77099
E: srijitmenon@kpmg.com

Dhirendra Kumar
Director,
Digital Trust
P: +91 78383 82665
E: dhirendrakumar4@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.

Acknowledgements:

- **Shagun**
- **Sakshi Kishore**
- **Rasesh Gajjar**
- **Arun Choudhary**