

# Fraud risks

## Evolving fraud risks in the “new normal” for life science organisations



At the onset of COVID-19, life science organisations were severely impacted by stringent nationwide lockdowns and constantly faced challenges across business operations, managing production and distribution networks.

Unavailability of employees at workplaces and travel restrictions largely disrupted supply chain and distribution systems. While a high surge in sales growth was visible during the second COVID 19 wave due to unprecedented demands of medicines, organisations also faced challenges in plant operations as multiple local regulatory approvals were required to ensure smooth movement of personnel and/or materials at site. Besides ramping up their production capacity and increasing work force, organisations had to adopt a flexible approach towards handling operations.

While compliance leaders remained fully committed in driving compliance through these times, a flexible approach had to be adopted by them to ensure seamless business support without affecting the adequacy of compliance programme.

### Areas where organisations had to adopt a flexible approach:

#### 1. Limited due diligence on vendors/suppliers/ third parties/employees/NGOs

- Expedited approvals to onboard vendor/ supplier/third party/employees/NGOs.
- Background checks on vendors/suppliers/ third parties/employees/NGOs were restricted to public domain checks at the time of approval.
- Enhanced due diligence involving site visits and gathering intelligence on the background of promoters/ beneficiaries/employees could not be performed on high-risk cases due to travel restrictions.

#### 2. Multiple hiring of vendors/ third-party intermediaries

- Increased workload pushed hiring of multiple third-party intermediaries for similar activities.
- Newly incorporated vendors were hired upon obtaining limited documents and information.

#### 3. Remote/ limited reviews

- Live/ on-site monitoring of charitable activities could not be performed to assess the end use of funds.
- Entity level Anti Bribery and Corruption (ABC) reviews were performed remotely, and limited documents were available for review to test effectiveness of compliance framework.
- Distribution channel partner monitoring reviews were performed remotely with restricted access to office and documents.

#### 4. Online training and awareness programmes

- In person trainings for employees and vendor/supplier/third party could not be done.



## Common fraud trends across life science organisations:

### 1. Procurement frauds: Employee and vendor potentially involved in misconduct through creative ways:

- a. Inexperienced vendors hired for cleaning, sanitisation, sterilisation, etc. in production department affecting manufacturing controls to prevent contamination of drugs.
- b. Employees colluded with existing vendors to procure materials/ services at a service margin to meet the high and immediate demands.
- c. Employees created entities in the name of relatives or friends.

### 2. Misappropriation of company's assets

- a. Theft of company's confidential, patented/ secretive and/or proprietary information by employees, whether or not in lieu of pecuniary benefits.
- b. Theft of inventory perpetrated due to reduced work force at premises.
- c. Misuse of company's assets or facilities such as use of car, guesthouse either for self-use or for government officials.

### 3. Distribution channel fraud risks

- a. Distribution of expired products, substandard, spurious, falsely labeled or counterfeit products by channel partners.

- b. Diversion of products to related parties and selling them at a higher price.

### 4. Regulatory and reputational fraud risks

- a. Reduced workforce at sites potentially impacted adherence to quality of current good manufacturing practice.

### 5. Hiring/recruitment frauds

- a. Misrepresentation of credentials by candidates: Validation of educational qualification from universities/ colleges and work experience from past employer could not be performed due to closure of offices.
- b. Candidates paying commission to recruiters to secure jobs.
- c. Collusion between hiring manager and recruiter to hire candidates in lieu of commission.
- d. Remote or hybrid working environment opened opportunities for employees to take up second job resulting in multiple risks for organisations such as conflict of interest, data leakage, low productivity, etc.

### 6. Cyber frauds

- a. Ransomware attacks and theft of data and intellectual property due to compromise of IT assets were continuously seen as high risks for life science organisations.



## How organisations can protect themselves?

Life science organisations are continuing with accelerated growth by driving new innovations, collaborations and digital transformation. Thus, organisations are engaged in – (i) setting up new infrastructure or upgrading existing facilities (ii) entering into joint ventures to manufacture medicines/clinical trials (iii) building up logistics distribution to meet regulatory requirement and (iv) reorganising marketing and sponsorship policies and procedures. It is imperative to strengthen existing controls and processes to address risk and challenges arising from new and evolving ecosystem.

Considering these recent developments, the immediate step is to investigate such instances focused on (a) identifying personnel involved, (b) establishing modus operandi adopted, and (c) identifying and remediating the underlying control gaps that translated into such fraudulent behaviour. The environment should be assessed on – culture and commitment at the top, existing internal controls and their adequacy in the current situation and robust monitoring reviews involving entity and third-party supplier/distributor.

### Some of the immediate better practices identified to tighten the controls and address risks are:



Fraud risk assessment: Using data analytics, identify risk profile of vendors and potential red flags correlating to similar issues prevailing



Data leakage prevention framework and periodic review



Onsite distributor reviews to assess the adherence of company's compliance policies



Conduct rapid investigations for cyber incidents to minimise exposure



Framework assessment of recruitment process and develop a framework for anti-fraud policies, systems and controls



Monitoring reviews for funds allocated to NGOs/charitable institutions



Anti-fraud workshops for finance/internal audit department to educate them on identifying early red flags while processing payments to vendors/supplier/distributors



## KPMG in India contacts:

### Vijay Chawla

#### Partner and Head

Risk Advisory

T: +91 80683 35509

E: vschawla@kpmg.com

### Jagvinder S. Brar

#### Partner and Head

Forensic Services

Risk Advisory

T: +91 97169 09339

E: jsbrar@kpmg.com

### Sudesh Anand Shetty

#### Partner

Forensic Services

Risk Advisory

T: +91 98203 60230

E: sashetty@kpmg.com

### Nupur Anand

#### Associate Director

Forensic Services

Risk Advisory

T: +91 99111 36260

E: nupuranand1@kpmg.com



[home.kpmg/in/socialmedia](https://home.kpmg/in/socialmedia)

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

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.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only. (020\_FLY1022\_PT)