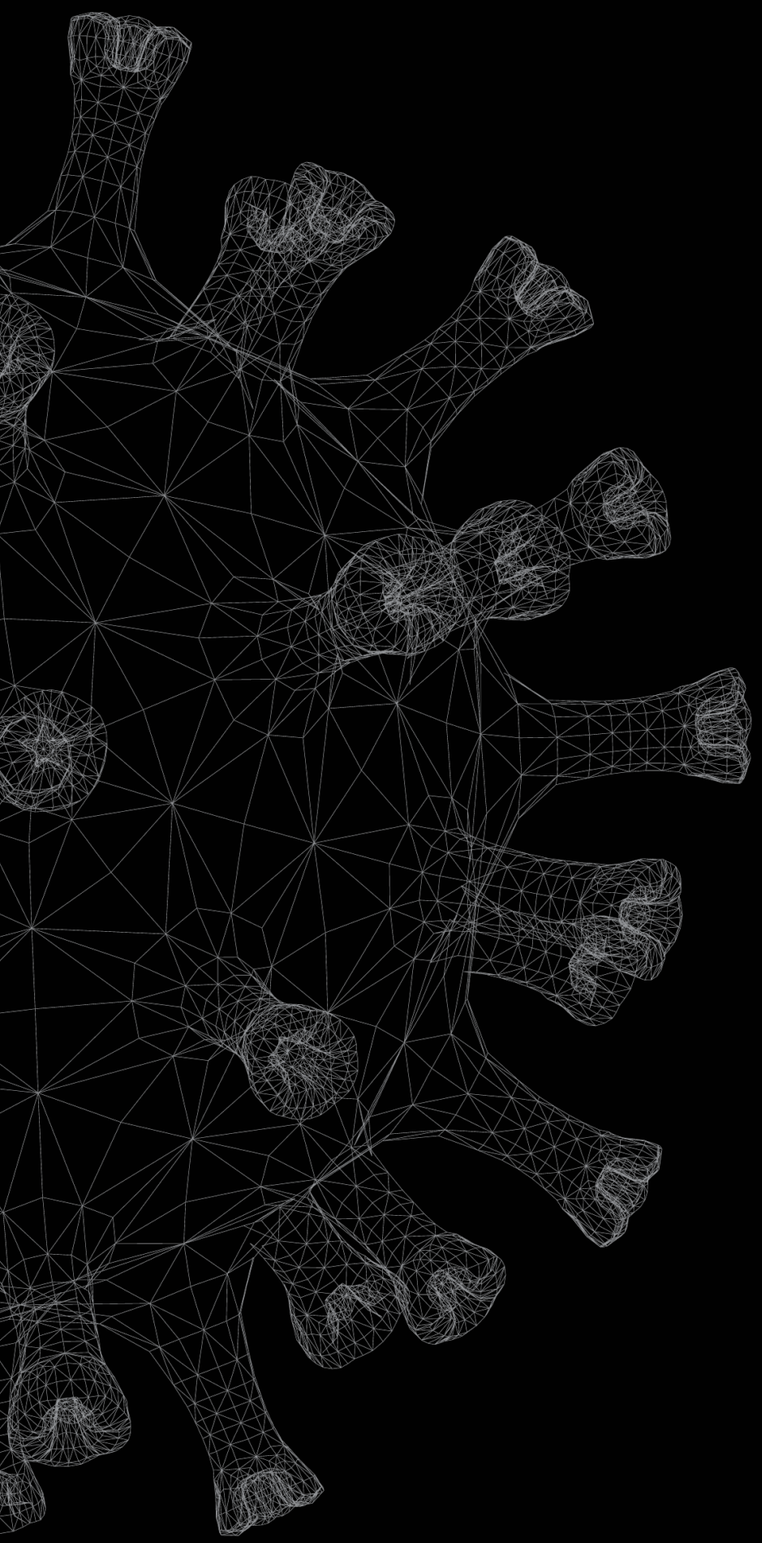
Deloitte.

Managing the risk of organisational fraud in the wake of COVID-19

A point of view

May 2020



Introduction

As companies operate on an unstable ground with changes in business modalities, relaxed controls, and new ways of working, they will also deal with new and increased vulnerabilities in certain avenues as a result of the new operating model and a stressed global economy. Organisations, and resultantly employees, are under pressure—the pressure of survival for businesses and performance for executives, financial pressure from accumulated debt and uncertain earning, anxiety and disgruntlement at possible pay cuts and job loss, and so on. Such pressure (a key element of the fraud triangle) may muddle one's perception of acceptable and unacceptable behaviour, manifesting in the actions of individuals within an organisation, as well as external parties such as vendors, partners, and customers. Such moments of vulnerability are also times when (unrelated) unscrupulous parties look to exploit unsuspecting organisations/individuals for personal benefit.

Historical data[1] also indicates that the recession that began in 2008, resulted in a significant increase in lawsuits based on fraudulent loss. It is possible that this may also happen with other companies/geographies in the current economic climate.

This document highlights some key considerations for organisations from a fraud vulnerability and preparedness standpoint during this time.

1 https://www.cio.com/article/2432203/lawsuit-increase-forecasted-due-to-economic-recession.html

Key fraud risks anticipated in the current crisis

FINANCIAL STATEMENT FRAUD

With financial pressure mounting on organisations, heightened by accumulated debt and reduced/uncertain earnings in the current situation, executives may feel the pressure to take desperate measures for averting corporate failure. The dependence of employees, vendors, and customers on the organisation may add to the rationalisation of such actions. Such pressure may percolate across levels and lead to fraud schemes resulting in financial misstatement. Instances include the following:

- Intentional delay/non-recording of losses or overvalue of assets to facilitate insurance recoveries
- Inflation of orders/sales to reflect increased revenues for fund raising or better share price/ valuations; understating expenses
- Override of existing internal controls, especially those critical to Internal Control over Financial Reporting (ICFR), in light of possibly relaxed monitoring and distractions
- Favouritism of client or supplier, including collection or payment waivers or prioritisation

SUPPLY-CHAIN FRAUD

Due to supply-chain disruptions, there are bound to be increased dependencies on existing vendors (who are able to fulfil requirements) and cultivation of new vendors (for meeting urgent requirements that existing vendors are unable to fulfil). These circumstances may give rise to vulnerabilities on account of the following:

- Bad actors masquerading as potential vendors looking to defraud organisations in the circumstances
- Inadequate due diligence on new third parties
- Favours sought by vendors to expedite/resume operations/emergency procurement under restricted conditions

Further, there may be vulnerabilities on the distribution side, which could lead to issues including inappropriate payments to distributors, payoffs to government officials to prevent disruptions in the distribution cycle, selling of counterfeit/ expired products.

TECHNOLOGY- AND DATA-RELATED FRAUDS

The sudden switch to a WFH model across businesses, especially with limited controls over network/data security, also poses a risk to organisations.

- Data theft, denial of services, or other forms of cyber attacks may occur due to perceived distractions in monitoring, limited controls around VPN due to remote access (WFH), and possible disgruntlement.
- Remote meeting security threats

CONTRACT FAILURES AND DISPUTES

- Vendor defaults – Failure/delay in fulfillment of contractual obligations, leading to disputes over payments. There may be instances of performance obligation defaults wrongfully attributed to COVID
- False claims or damage submissions by customers/ vendors on account of business disruptions

OTHER CORRUPT PRACTICES

Insider trading – In the current situation, companies may struggle to identify and control the flow of non-public information. Compounding the situation are remote employees, which makes monitoring the use of confidential information difficult. Financial pressure and perceived opportunity may give rise to insider-trading risks

Managing the risk of organisational fraud in the wake of COVID-19

Best practices to be followed by organisations to eliminate these fraud risks

ORGANISATIONAL TONE

"Tone at the top" refers to the ethical atmosphere that is created in the workplace by an organisation's leadership.

What can you do?

- Reiterate the tone at the top that compliance is a priority through mailers and training programmes on code of conduct and anti-corruption.
- Address fraud considerations as a result of the current pandemic, such as fraud mitigation and preparedness for incident response.
- Realign policies to reflect temporary/long-term disruption in business, data integrity, and confidentiality considerations with people working from home and value chain.

Checklist to relook at fraud preparedness

- How are existing controls including those on financial reporting impacted by the changed business environment?
- Are new controls required?
- Does your organisation reward whistle-blowers in good faith?
- How will heightened corruption and fraud risks be addressed in third-party interactions/contracts?

HOTLINE AND REPORTING MECHANISM

Step up employee education and awareness regarding the hotline and matters that should be reported. Sensitise them to current pressures.

What can you do?

- Coach employees on managing performance pressure, reinforce identifying unacceptable business practices (reporting on the hotline), which is especially relevant given the pressures created by the pandemic.
- Reiterate the importance and use of hotlines.
- Communicate the attributes of the WB channel including confidentiality to reduce the fear of retaliation.
- Track and analyse metrics of report information.

Checklist to relook at fraud preparedness

- Are staff/third parties empowered to bring issues to the attention of the company?
- Does your organisation have a response plan in place for issues reported through the hotline?
- Do you have the necessary infrastructure and preparedness to conduct investigations remotely (including discovery, gathering email data, device data, and logs)?

TECHNOLOGICAL PREPAREDNESS

Technological preparedness is imperative for organisations to face evolving cyber risks due to the impact of the pandemic and increased use of remote working and be prepared for remote investigations.

What can you do?

- Assess infrastructure readiness to support remote access and download ERP data, enterprise data from server/cloud storage; check activation of relevant logs.
- Assess the enterprise collection capability for remote access to custodian devices.
- Set up secure data rooms for sharing confidential data.

Checklist to relook at fraud preparedness

- Communicate best practices to employees such as using company-approved storage and expecting increase in phishing attempts with COVID-19 related topics.
- Step-up data/network security with remote employees' home networks with limited security.

STRENGTHEN DUE DILIGENCE

Conduct a comprehensive study of a business undertaken to establish its assets and liabilities and evaluate its commercial potential.

What can you do?

- Assess third-party risks to business continuity.
- On-board new third parties subject to necessary declarations and approvals.
- Assess existing supplier contracts to determine risk exposures.
- Assess the impact of alternative supplier/distribution networks.

Checklist to relook at fraud preparedness

- Identify high-risk/critical third parties (dependency on business, geographical location).
- Recognise how equipped your organisation is in conducting remote due diligence as opposed to on-site diligence.
- Create a plan to fulfil obligations for due diligence for emergency procurements.

ASSESS/PREPARE FOR POTENTIAL DISPUTES/LITIGATION

The pandemic can disrupt businesses due to increased commercial and financial risks.

What can you do?

- Review contracts with third parties to assess direct/indirect financial implications of non-performance by either party or delays as a result of the pandemic.
- Establish plans/procedures in place to identify, preserve, collate, and analyse the evidence and data (for example, email correspondence).

Checklist to relook at fraud preparedness

- Has the impact of COVID-19 created or exacerbated a contractual under performance (or might in the future)?
- What is the financial impact on your business and on the rest of the supply chain from failing to meet obligations?

REGULAR MONITORING

Implement regular monitoring and enhanced focus on the financial-statement compilation process, especially for high-value/sensitive transactions, to identify red flags.

What can you do?

- Establish a mechanism to monitor new vendors, high-value/sensitive transactions to ensure timely action is taken in case of red flags.
- Prepare adequate disclosures in case you assess COVID-19 as a material event.
- Extend audit of transactions during COVID-19 to identify issues in advance of the FS compilation process.

Checklist to relook at fraud preparedness

- Assess the impact of COVID-19 on estimates and judgements inherent in financial reporting.
- Assess necessary provisions relating to impairment of assets and inventory valuation.
- Foreign exchange volatility – recognise if additional hedging instruments will be needed to mitigate this risk.

Managing the risk of organisational fraud in the wake of COVID-19

One of the reasons that fraudsters are successful in times of crisis is because companies are usually focussed on dealing with immediate issues, and corporate governance aspects may at times take a back seat. It is important to be aware of your fraud risks, have robust systems in place, and remain vigilant during the crisis to mitigate fraud losses and associated potential reputational damage, and be adequately prepared to detect and address such concerns that may emerge in a timely manner.

Acknowledgements

We would like to thank Kasmera Shah, Kruthika More, and Aishwarya Venturapalli for contributing to this document.

Key Contacts

NIKHIL BEDI
Partner, Leader
Forensic, Financial Advisory
Deloitte Touche Tohmatsu India LLP
nikhilbedi@deloitte.com

ROHIT GOEL
Partner
Financial Advisory
Deloitte Touche Tohmatsu India LLP
rogoel@deloitte.com

ARJUN RAJAGOPALAN
Partner
Financial Advisory
Deloitte Touche Tohmatsu India LLP
rarjun@deloitte.com

KAVITA NATHANIEL
Director
Financial Advisory
Deloitte Touche Tohmatsu India LLP
knathaniel@deloitte.com

Deloitte.