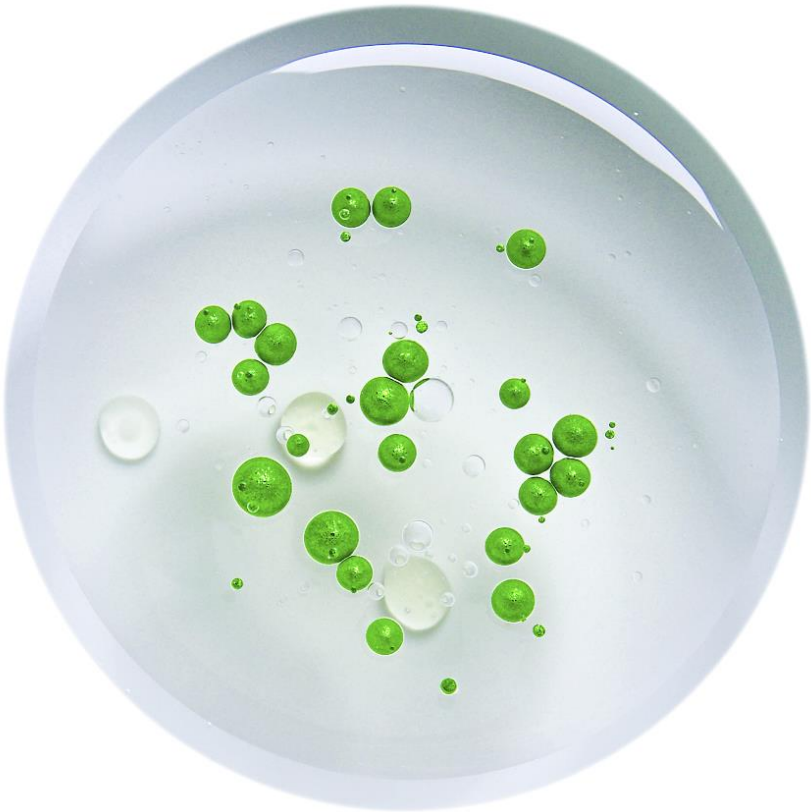
Deloitte.



The impact of COVID-19 on the **fraud risks** faced by organisations

The emergence of the COVID-19 pandemic and related government shutdowns has placed a lot of business operations under immense pressure. Organisations and their employees are now faced with increased fraud exposures and in addition it has presented organisations with new compliance related challenges.

The rapid changes also affect companies' control environments, bringing new opportunities for potential internal or external fraudsters. There is no doubt that the overall pressure on employees is increasing and they might be presented with easier rationalization of their non-compliant behavior. We believe that the theory will unfortunately become reality in this case and overall the incidents of fraud will increase in numbers.

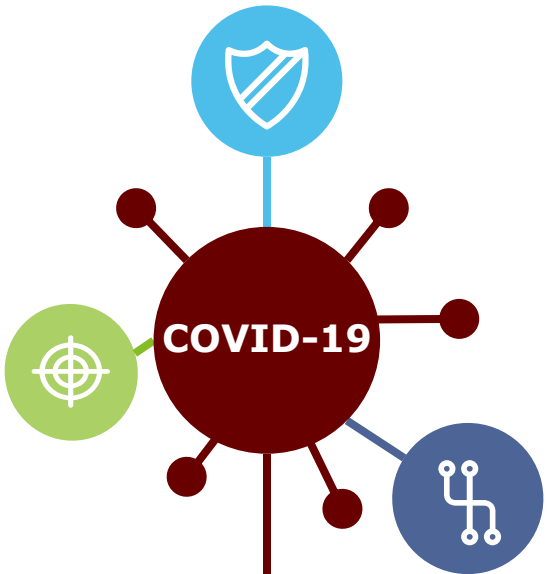
Significant **threats** and **fraud risks**

Supplier channel disruption and third party due diligence failures

An immediate challenge is the disruption of supplier channels on a global scale, creating an urgent need for supply network mapping in order to address various market scenarios. Essential procurement has to be localized quickly due to Covid-19 related lockdowns and restrictions, in addition many organisation's internal controls are under intense pressure increasing the risk of standard procurement control circumvention.

Missing key employees from workforce

With the epidemiological risk we have seen a lot of crucial employees work from home and in some situations employees have been absent due to the strict enforcement of quarantines by authorities. Organisations need to protect themselves by mitigating the impact that absent crucial employees will have on operations. Remote work increases the risk of confidentiality leaks.



Financial statement fraud

As many businesses are not operating at normal levels, the risk that organisations will mis-represent the impact of the pandemic on their financial records is increased. Also, the situation might provide a good opportunity for the hiding of previous mis-management or mis-appropriation of assets. In addition, organisations now have an increased incentive to misrepresent the nature of their businesses in order to qualify for certain government subsidies.

Old scam, **new** coat!

CEO fraud

The crisis mode makes it easier for fraudsters to target employees by sending "urgent" emails pretending to be from members of senior management, leading to employees disclosing information or wiring money.

Fraudulent products and services

Organizations are equipping their employees to work safely from home by purchasing devices, software and tools to allow for home office work. Such purchases are often made under time pressure. Thus, the organizations are more vulnerable to the risk of fraudulent purchases of equipment and software.

Insolvency fraud

With likely increased numbers of insolvency proceedings, we expect new forms of false claims and creditor-favoring schemes to appear.

Phishing and other information security threats

The current mode of operations may also make employees more susceptible to scams like (spear)phishing, vishing and zoombombing. This is at the same time that companies are also undergoing quick internal changes, potentially limiting the effectiveness of their IT Security tools and environment.

Misappropriation of assets and theft

The focus on business operations, coupled with vast numbers of staff working from home, has left the controls which protect the assets of organizations more vulnerable than they typically would be (to both internal and external fraudsters).

We are happy to advice and help with awareness.

How can we **help** you?

We provide **business intelligence services** – an efficient way to assess the risks connected to potential new suppliers organizations urgently need to onboard, but do not have required capacities or information sources for such **background checks**. We can highlight for you potential issues – providing inputs into your **third party risk management** and decision-making processes.

Similarly we can perform background checks on individuals in form of **pre-employment screening** in case you need to urgently hire larger number of new employees (as substitution or because the situation fuelled your growth). The screening includes verification of employment history, business activities, adverse press releases, criminal history, presence on sanction lists.

Our experienced colleagues **might step in to help temporarily** your teams **performing key and regulatory controls** and checks if they become incapacitated or significantly effected. At the same time we would be looking for optimization opportunities.

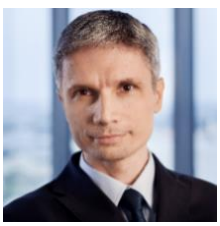
If needed this can be transformed into **outsourcing** of the processes and duties.

You might be considering changing some of your **processes involving physical contact** with customers or suppliers, for example using remote identification. We can assist with the **regulatory aspects and managing fraud risks** associated with the new solution.

Later, you might discover a **suspicion of fraud** or other misconduct rooted in the current situation and its negative impact on controls. We will be ready to provide flexible **advice on what investigative steps** to take and to deploy our modern **forensic technologies** for example to increase chances of **recovery**.

Contacts

Aaron Goldfinch
Partner
Forensic Practice Leader
+48 662 155 399
agoldfinch@deloitteCE.com



Mariusz Bereśniewicz
ACCA, CFE, CIA
Manager, Forensic
+48 539 978 894
mberesniewicz@deloitteCE.com

MAKING AN IMPACT THAT MATTERS since 1845

Deloitte.