

Managing Risks with Coronavirus

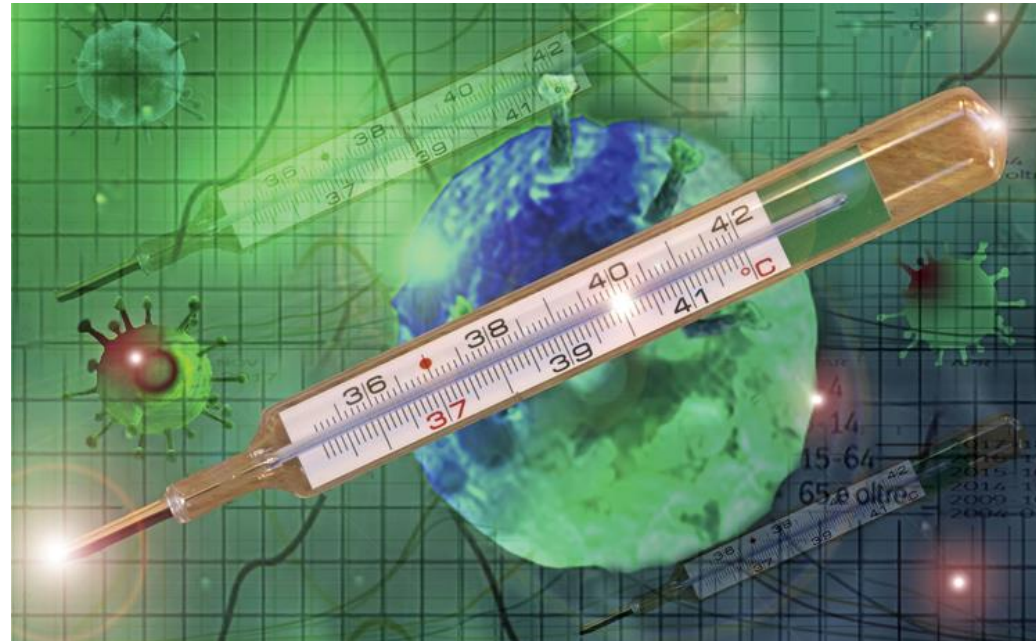
Doron Rozenblum, Managing Partner

How will your organization generate revenue and conduct business with organizations and clients either off-line or remotely?



Six Business Risks

Here are some of the key risks that organizations face as the COVID-19 crisis deepens.



Risk 1: Disruption Due to Social Distancing

Social distancing is a term applied to certain actions that are taken by public health officials to stop or slow down the spread of a highly contagious epidemic.

- Most business events and travel are cancelled during this peak period and potentially for an extended undefined period afterwards.
- How will your organization generate revenue and conduct business with organizations and clients, mostly off-line or remotely?

Risk 2: Decline in Employee Productivity

Every industry will be impacted.

Over 40% of staff during this period may be unable to work due to closure, sickness, either directly or indirectly.

Even if your employees are not infected, many will be affected by the need to care for family members, and be stressed or in bad mood.

They may also need flexible working hours due to school and daycare closings.

Risk 3: Stressed Supply Chains

The global economy is still highly integrated and most countries and companies rely on vendors for their business. From pharmaceutical raw materials to electronics to most consumer-good products, there will likely be **purchasing delays**. Heavy equipment and manufacturing **supply chains are already being impacted by COVID-19 spreading globally**.



Risk 4: Recession, Unemployment and Investment Pull-back

- Forecasts indicate that we will likely be in a recession by the fourth quarter.
- Consumers reduce and are extremely conscientious about their spending.
- Corporations are asking people to work from home.
- Watch the hospitality industry for signs of economic health.
- Investments are highly negatively impacted by uncertainty and corporations will likely cut back expansion and growth investments, contributing to a rapid rise in unemployment.
- There may be significant layoffs at existing businesses.

Risk 5: Economic Instability and Civil Unrest

- Budget deficit is at a record high.
- Government spending will ramp-up, but that may not be effective due to lack of planning and preparedness.

Risk 6: Cyber risks and fraud risks

Cyber criminals may take the opportunity to increase **distributed denial of service** attacks on certain banks' websites and send out **phishing** emails.

Depleted staff at call centers increases the risk of account fraud if criminals take their chance when the chaos is at its peak.

Due to the COVID-19 crisis and the drastic measures that governments and companies have taken, a significant increase in fraud risks becomes apparent.

The main reason is an extremely **vulnerable control environment**.

Deviation from checks and controls **normally** included in the process.

Increased caution is required regarding the already proven effective methodology of "CEO fraud".



Organizations need to put in place mitigation plans to address each of these risks. By taking these steps they will be in a better position to reduce the risks that the coronavirus will have on their business.

The mitigation activities that your business can establish and implement can range depending on your industry, geography, size, and other factors.

These initiatives may include activities such as shifting budgeting from fixed costs to variable spending to provide flexibility in times of uncertainty.

Six risk management steps that organizations should think about as they defend themselves against the pandemic effects.



Step 1: Readiness Assessments

A readiness assessment is a good place to start when organizations are not sure what their business continuity program should include.



Step 2: Risk Management Plan

All organizations should complete a risk assessment on their core business processes to identify and prioritize any new risks or gaps in their existing controls for new scenarios like pandemics, recession, and geopolitical conditions risks. Managers on the front line when prompted with risks are in the best position to be able to assess how these scenarios will impact their areas of responsibility.

Step 3: Business Impact Analysis

A business impact analysis allows organizations to identify which parts of the business are most critical to its operations.

Use the results to determine which parts of the organization to prioritize during a business continuity plan event to maintain operations.

Step 4: Policy and Procedure Management

As the pandemic evolves and new information arises, policies and procedures will need to be revisited and updated and communicated. For example, reviewing and revising a work-from-home policy and checking its effectiveness.



Step 5: Incident Management

Incident management is typically embedded within a process.

Incident Management aims to manage the lifecycle of all Incidents (unplanned interruptions or reductions in quality of IT services as an example).

The primary objective of this process is to return the service to its users as quickly as possible..



Step 6: Cyber and Fraud Awareness

CYBER

- Cyber health check\risk assessment
- Cyber awareness training for employees
- Phishing software
- SOC – Security Operation Center services

FRAUD

- Are key controls in the primary processes covered?
- What additional controls should be considered regarding exposure to external influences?
- Is there sufficient IT capacity to facilitate the tasks that are usually handled offline?
- How is the performance of checks and controls monitored when employees work from home?



Thank you!



Doron Rozenblum, Managing Partner



EZRA YEHUDA - ROZENBLUM
Consulting, Control & Risk Management

The Levinstein Tower, 5th floor ■ 23 Menachem begin road, Tel Aviv 6618356, Israel
Tel. +972-3-6130-632 ■ Fax. +972-3-6130-637
office@kreston.co.il ■ www.kreston.co.il