

## TECHNOLOGY

# COVID-19 Practical Considerations: Business Continuity Planning

23 April 2020

The ongoing COVID-19 situation has placed business continuity plans (“BCPs”) in sharp focus for organisations across a wide range of industries.

## KEY CONTACTS



**Colin Rooney**  
Partner  
+353 1 920 1194  
colin.rooney@arthurcox.com



**Ian Duffy**  
Associate  
+353 1 920 2035  
ian.duffy@arthurcox.com

Many organisations have been able to call on sophisticated BCPs to assist with mitigating the impact of COVID-19 but this has not been a universal experience. While it may now be difficult for some organisations to develop and implement a robust BCP in time to help with their current response to COVID-19, the ongoing COVID-19 pandemic should serve as a pertinent reminder of the important role that sound business continuity planning plays in operational resilience.

In this briefing, we provide an overview of sound business continuity planning which organisations should bear in mind when reviewing their existing business continuity arrangements and contracting with key service providers in the future.

## What is business continuity planning?

Business continuity planning involves the development, maintenance and implementation (where necessary) of processes and procedures which are designed to minimise the impact of disruptive incidents, such as COVID-19, on an organisation's business so that the organisation may continue to function notwithstanding the occurrence of a disruptive incident.

## Key steps for effective business continuity planning

There are a number of key steps that are

inherent in effective business continuity planning for most organisations. We summarise these key steps below:

- 1. Critical resources** – an organisation should identify the critical resources on which it is dependent. These resources might include IT systems (including cloud systems), communications systems, buildings and personnel.
- 2. Disruptive incidents** – an organisation should identify the types of disruptive incidents that could impact the organisation's critical resources. These disruptive incidents could include severe weather events, public health emergencies (such as COVID-19) and wars.
- 3. Impact of disruptive incidents** – an organisation should assess the potential impact of disruptive incidents on the organisation's business (and in particular, its critical resources). This impact could be operational, financial, legal or reputational in nature.
- 4. Recovery Priorities and Objectives** – an organisation should analyse the information gathered based on steps 1 to 3 to assist it in defining the organisation's recovery priorities and objectives upon the occurrence of a disruptive incident. These priorities and objectives could include the sequential order in which critical resources need to be recovered or maintained

and the level of functionality that an organisation will need to maintain in its critical resources to continue to function at an acceptable level during a disruptive incident.

**5. Development of BCP** – an organisation should use the outcomes of steps 1 to 4 to help it build the policies and procedures that make up its BCP. These policies and procedures will be designed to provide the organisation with a comprehensive playbook for effectively responding to a disruptive incident and minimising its impact on the organisation’s business.

**6. Investment in Personnel and Infrastructure** – the BCP may, by itself, be of limited use if it is not supported by appropriate investment in personnel and infrastructure. The organisation should ensure that relevant staff are aware of the BCP and the role that they must play to ensure that it is effective. Appropriate staff training can assist in this regard. Organisations must also ensure that effective investment is made in its infrastructure so that

the BCP can be effectively deployed if this becomes necessary. By way of example, such investment might be in an organisation’s remote working capabilities.

**7. BCP Testing** - the BCP should be subject to periodic testing (e.g. annual) to ensure that it remains ‘fit for purpose’. The organisation should also ensure that it takes action to address any deficiencies in the BCP that are identified through this testing.

**Role of service providers in effective business continuity planning**

For many organisations, ensuring that they have in place their own robust BCPs may not be sufficient (of itself) to effectively minimise the impact of a disruptive incident on their business. Where service providers are used by an organisation to provide functions or services that are critical to the ongoing operation of that organisation, it will also be important to ensure that those service providers have in place their own robust BCPs.

Similarly to an organisation’s own BCP, a critical service provider’s BCP should be designed to minimise the impact of disruptive incidents on the service provider so that it may continue to provide the relevant services to the organisation notwithstanding the occurrence of a disruptive incident. The most effective way for an organisation to obtain appropriate assurance around the business continuity planning from its critical service providers is through appropriate contractual commitments.

More specifically, the organisation’s contract with the critical service provider should require the service provider to develop and maintain a robust BCP. The service provider should also be subject to a contractual obligation to periodically test its BCP and update it where necessary. The organisation may also wish to consider specifying certain circumstances where the critical service provider’s BCP should be deployed.

*We would like to thank Sonam Gaitonde for her contribution to this article.*