How to Think About **Business Continuity** In Relationship to Your Third Parties

No doubt you have put a lot of time, thought and resources into your own Business Continuity plan and testing. And for good reason.

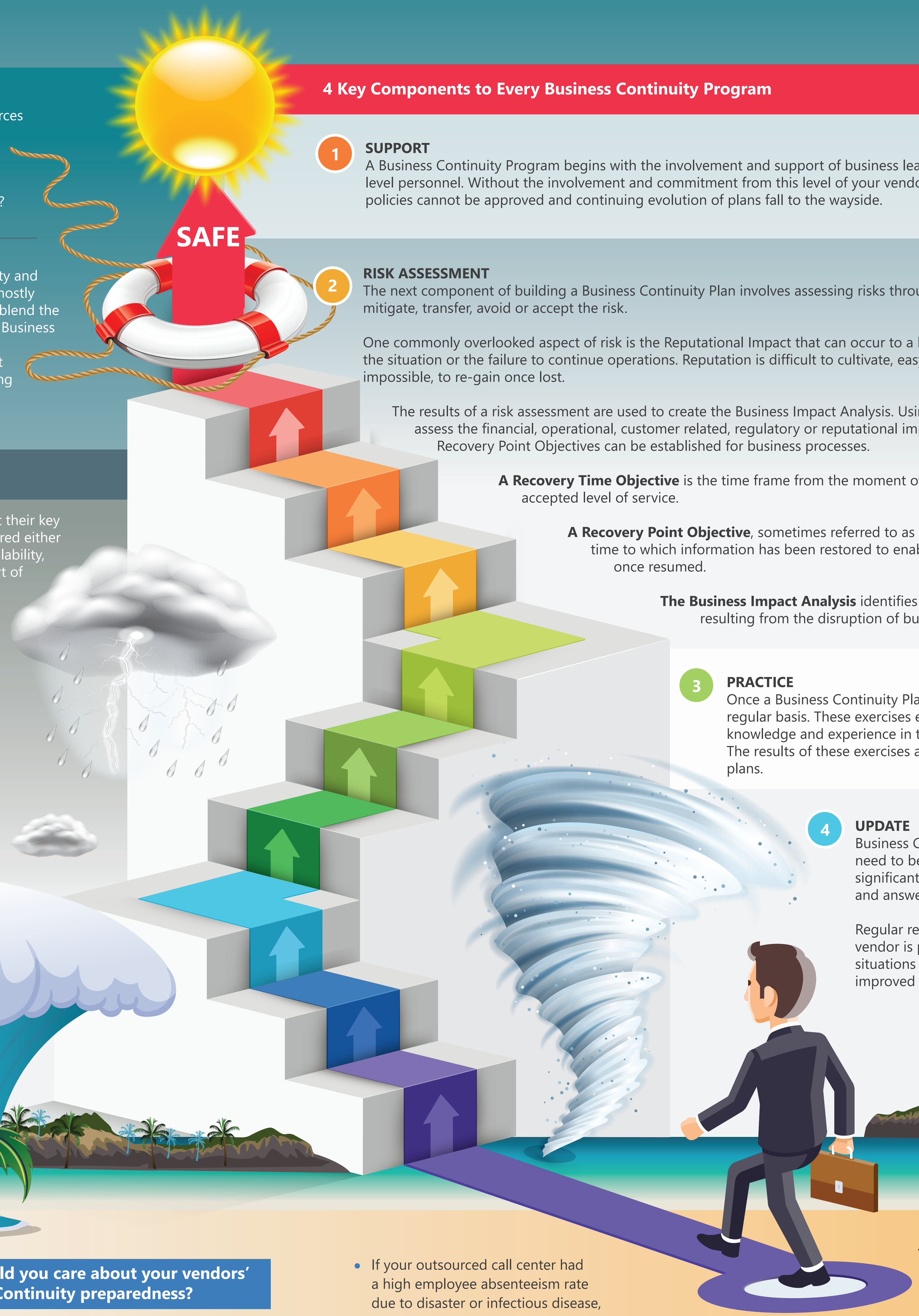
BUT.....have you replicated that effort when it comes to assessing the same for your critical third party providers?

Let's start with the difference between Business Continuity and Disaster Recovery. Many people confuse the two terms mostly because of the plethora of online resources that tend to blend the two together. For clarity, Disaster Recovery is a subset of Business Continuity that addresses the immediate response to a business impacting event. We'll come back to the subject of Disaster Recovery in a future release. Today, we're going to focus solely on Business Continuity. Let's get started.

What is Business Continuity?

Business Continuity allows for businesses to ensure that their key operations, products and services continue to be delivered either in full or at a predetermined, and accepted, level of availability, normally outlined in a Service Level Agreement as a part of your vendor contract.

Includes: planning for loss of personnel, facilities or services; planning with public entities such as emergency services, local or state disaster relief agencies; and communications with identified key vendors, clients, employees and the media.



4 Key Components to Every Business Continuity Program

1 **SUPPORT**
A Business Continuity Program begins with the involvement and support of business leaders, such as senior level and or board level personnel. Without the involvement and commitment from this level of your vendor's organization, funding is not available, policies cannot be approved and continuing evolution of plans fall to the wayside.

2 **RISK ASSESSMENT**
The next component of building a Business Continuity Plan involves assessing risks through a risk analysis and deciding to mitigate, transfer, avoid or accept the risk.

One commonly overlooked aspect of risk is the Reputational Impact that can occur to a business from the failure to respond to the situation or the failure to continue operations. Reputation is difficult to cultivate, easy to lose and very hard, if not impossible, to re-gain once lost.

The results of a risk assessment are used to create the Business Impact Analysis. Using standardized criteria to measure and assess the financial, operational, customer related, regulatory or reputational impacts, Recovery Time Objectives and Recovery Point Objectives can be established for business processes.

A Recovery Time Objective is the time frame from the moment of disruption to the return to an accepted level of service.

A Recovery Point Objective, sometimes referred to as Maximum Data Loss, is the point in time to which information has been restored to enable the business function to operate once resumed.

The Business Impact Analysis identifies the operational and financial impacts resulting from the disruption of business functions and processes.

3 **PRACTICE**
Once a Business Continuity Plan is created, it needs to be exercised on a regular basis. These exercises ensure that everyone involved in the plan has knowledge and experience in the activities they will be required to perform. The results of these exercises allow a business to adjust and improve their plans.

4 **UPDATE**
Business Continuity Plans and the Business Impact Analysis need to be reviewed and updated regularly or when significant change occurs within an organization. New risks and answers to those risks emerge and evolve constantly.

Regular reviews, along with plan exercises, assure that the vendor is prepared and able to respond to whatever situations arise and allow the corresponding plans to be improved to minimize the impact of the event.

Why should you care about your vendors' Business Continuity preparedness?

With the interconnected nature of products and services offered by organizations through third-party relationships, having any part of the organization's services becoming unavailable for an undetermined amount of time could significantly impact operations and reputation. Organizations benefit from knowing how quickly vendors plan to recover from certain business impacting events, how much data could be lost due to that event and that their vendors will survive a business impacting event.

- If your outsourced call center had a high employee absenteeism rate due to disaster or infectious disease, do they have staffing replacement plans in place to continue to provide satisfactory customer service? If your core banking provider lost its primary office due to a hurricane, do they have office space, furniture, computers and telecommunication connections ready in another location? Are the displaced employees able to move locations and perform the same capacity of duties?
- Your online banking provider is victim of a cyber-attack leading to the exposure of four million customer records. Is your vendor ready to respond with a communications plan and a designated public speaker? Do they have a plan in place to sustain the reputational impact? Did they contact you to tell you about it, or do you have to contact them to explain after it's on the news?

Ensuring that your critical vendors can survive in the face of disruption helps ensure that your business can also survive.

Venminder has a team available to do a qualified BCP/DR review and analysis.
Download a free sample of our BCP/DR Analysis now.

DOWNLOAD NOW

venminder
400 Ring Road, Suite 131, Elizabethtown, KY 42701 | (270) 506-5140
www.venminder.com