BUSINESS CONTINUITY PLANNING: HOW TO CREATE AND MAINTAIN BCPS

The COVID-19 pandemic has brought to the surface a lot of misconceptions and, frankly, unpreparedness on the part of many organizations to handle disruptions to normal business operations. Writing for Risk.net, Ariane Chapelle states that pandemic risks are sometimes called 'grey rhinos': probable, high-impact trends that are clearly observable, but often ignored until it's too late.

So many organizations have been caught flatfooted, unable to consider a situation where their staff must work from home, and their supply chains and customer demand are interrupted. There's also the inability to predict a return to normal. They haven't had a plan for business continuity.

But, fortunately for us, there are companies we can reference as good examples of how business continuity planning should be done. Let's take a look.

What is business continuity planning?

The ISO 22300:2018 vocabulary publication on Security and Resilience defines a **business continuity plan (BCP)** as documented information that guides an organization to respond to a disruption and resume, recover, and restore the delivery of products and services consistent with its business continuity objectives. BCPs provide guidance and information to assist teams to respond to disruptions and assist the organization with making the right response and ultimately recovery from the disruption.

As a BCP is a reference to be used during disruptions, it is best that your organization agrees to a single format for the document as well as, importantly, where the BCP is kept. Excellence in business continuity planning is based on two components:

1. That your BCP plans can be accessed no matter the disruption.
2. That your plans are easily understood by all relevant stakeholders involved in the response and recovery activities.

Use of secured cloud file shares that are hosted by different providers in different regions offers the best option in terms of accessibility, updating, and security. However, you must also consider if the internet is down. Having a hard copy version stored somewhere outside normal business premises would be an ideal backup, though keeping it updated needs a significant amount of discipline.

Creating a business continuity plan

Step 1: Perform risk assessment & business impact assessment

When it comes to business continuity planning, the first stop is to perform **risk assessment** and **business impact assessment (BIA)** activities. Risk assessment involves:

1. Identifying potential risks based on the organization's business environment.
2. Analyzing these risks in terms of probability, impact, and proximity.
3. Evaluating these risks from a priority perspective.
4. Determining the appropriate risk treatment measures such as avoiding, accepting, reducing or sharing the risk with third parties.

A good example is Wimbledon, which updated its insurance policy to include infectious disease clauses following the outbreak of SARS in 2002. The organization is set for a potential $141 million payout following cancellation of the 2020 tennis tournament due to COVID-19.

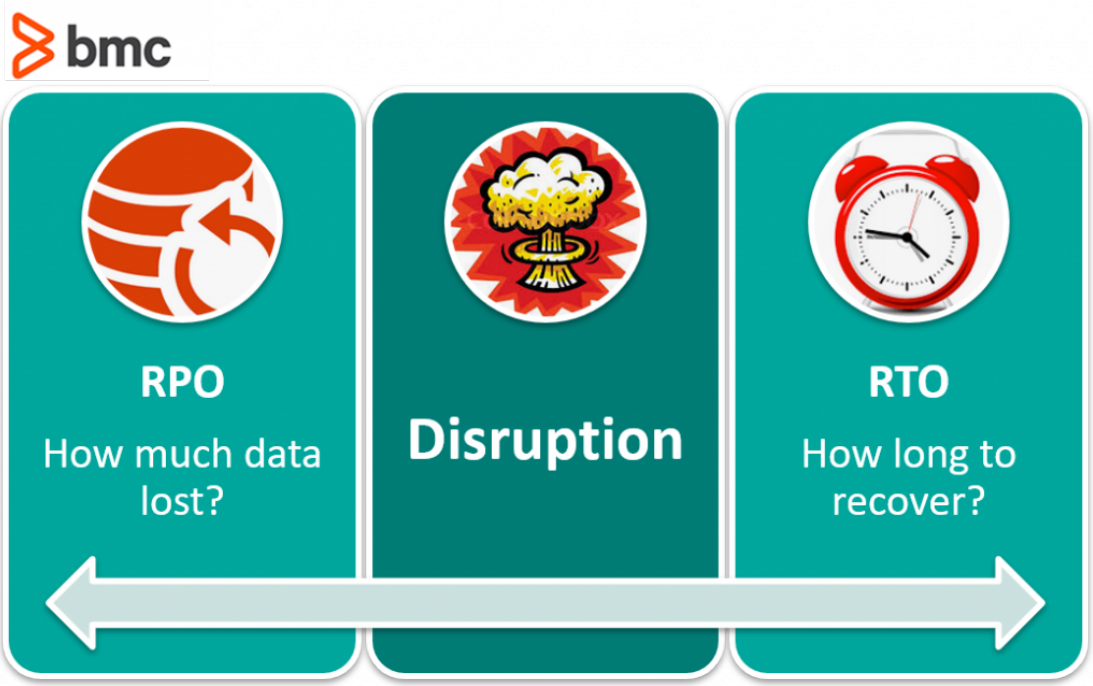
During the BIA phase, the organization takes these actions:

1. Defining types and criteria of impact based on the organization's business environment.
2. Identifying key business process activities.
3. Determining impact of disruption based on the types and criteria defined earlier.

A key output is the maximum time length that the organization can bear the disruption and, as a result, determination of the prioritized timelines for resuming business operations following the

disruptions. The measures for these prioritized timelines are:

- **Recovery Point Objective (RPO)** for allowable data loss based on time
- **Recovery Time Objective (RTO)** for the time to restore business processes



Determining prioritized timelines for resuming business operations following a disruption

BIA activities are very critical for any organization wanting to understand the cost of disruption, and then plan the prioritized approach for dealing with the disruption.

Step 2: Develop business continuity strategies

The outputs of the risk assessment and BIA activities feed into your **business continuity strategies** which consider the options before, during, and after disruption, and determine the right solutions. The choice of strategy is based largely on how much loss your organization is willing (or able) to take as well as the amount of resources it is willing to pour into the available options.

These strategies and solutions should consider how to meet the BIA timelines, decrease risk probability and impact, and reduce the duration of the disruption. For example, your solutions might include:

- Creating a succession plan for a people risk perspective
- Deploying backups and disaster recovery solutions for technology and information risks
- Remote working for office access risks
- Engaging multiple suppliers to limit supply chain risks

Step 3: Document business continuity plans

Based on the selected strategies and solutions, you'll then document your BCPs and make them available to key stakeholders. According to the ISO 22301:2019 standard on business continuity management systems requirements, BCPs should:

- Include specific immediate steps to be taken following a disruption

- Be flexible enough to respond to changing conditions of a disruption
- Focus on the impact of incidents that potentially lead to a disruption
- Be effective in minimizing impact of disruptions
- Assign roles and responsibilities for tasks within a disruption

The structure of a BCP would therefore include:

a. Purpose, scope, and objectives
b. Roles and responsibilities
c. Actions to implement solutions
d. Supporting information needed to activate, operate, coordinate, and communicate actions
e. Internal and external dependencies
f. Resource requirements
g. Reporting requirements
h. Process for standing down (i.e., return to normal)

Maintaining BCPs

A BCP is as good as dead if no effort is taken to train stakeholders and constantly review whether it is effective to meet the ever-changing threat landscape that faces your organization.

Two ongoing activities are essential to maintaining your BCPs: ensuring that testing and training are part and parcel of the business continuity planning activities. Then, management must regularly review the outcomes of this testing and training.

Testing your BCP

Testing is an integral part of maintenance and should be regularly planned and carried out based on the risk profile. The scope of testing can be anything from table-top exercises to full-scale exercises, but you must ensure that your testing activities do not significantly impair normal business operations.

Only by regular testing can a business truly know whether it can meet the RTO and RPO targets when an actual disruption occurs. Where the tests reveal otherwise, then the organization can take the right steps to remedy the situation by allocating relevant resources as appropriate to keep the BCPs actionable, reliable, and updated.

Training around your BCP

Coupled with testing is the need for training and awareness. Business continuity and disaster recovery procedures are only useful if *all* the members of the team are aware of where to access and how to execute them when a disruption occurs. You'll want to create drills for employees to participate in to practice. Additionally, a strong knowledge sharing culture is vital for a BCP to be successful.

No BCP? Plan to fail

The old adage "failing to plan is planning to fail" comes to mind whenever one thinks of BCP. Statistics from FEMA reveal that roughly 40-60% of small businesses never reopen their doors

following a disaster. In addition, 90% of smaller companies fail within a year unless they can resume operations within five days following a disaster. By comparison, 20% of larger companies spend over 10 days per month assessing their continuity plans.

The COVID-19 pandemic, and many similar disruptions, clearly indicate that organizations that don't take time to plan for disruptions are the ones hardest hit. They're the same organizations that will take longer to recover than competitors who are better prepared.