Business Continuity Workbook

Strategizing to mitigate risks from unexpected events is at the core of business continuity management. An effective strategy starts with getting your ideas formalized.

Use this workbook to help build out a:

- Risk assessment that identifies potential sources of business disruption
- Business impact analysis that outlines the costs of a disruption
- Disaster recovery plan for your key systems, data and applications
- Business continuity plan for your critical business processes

Ultimately, this workbook gives you the tools to put your business continuity strategies into words that lead to action.

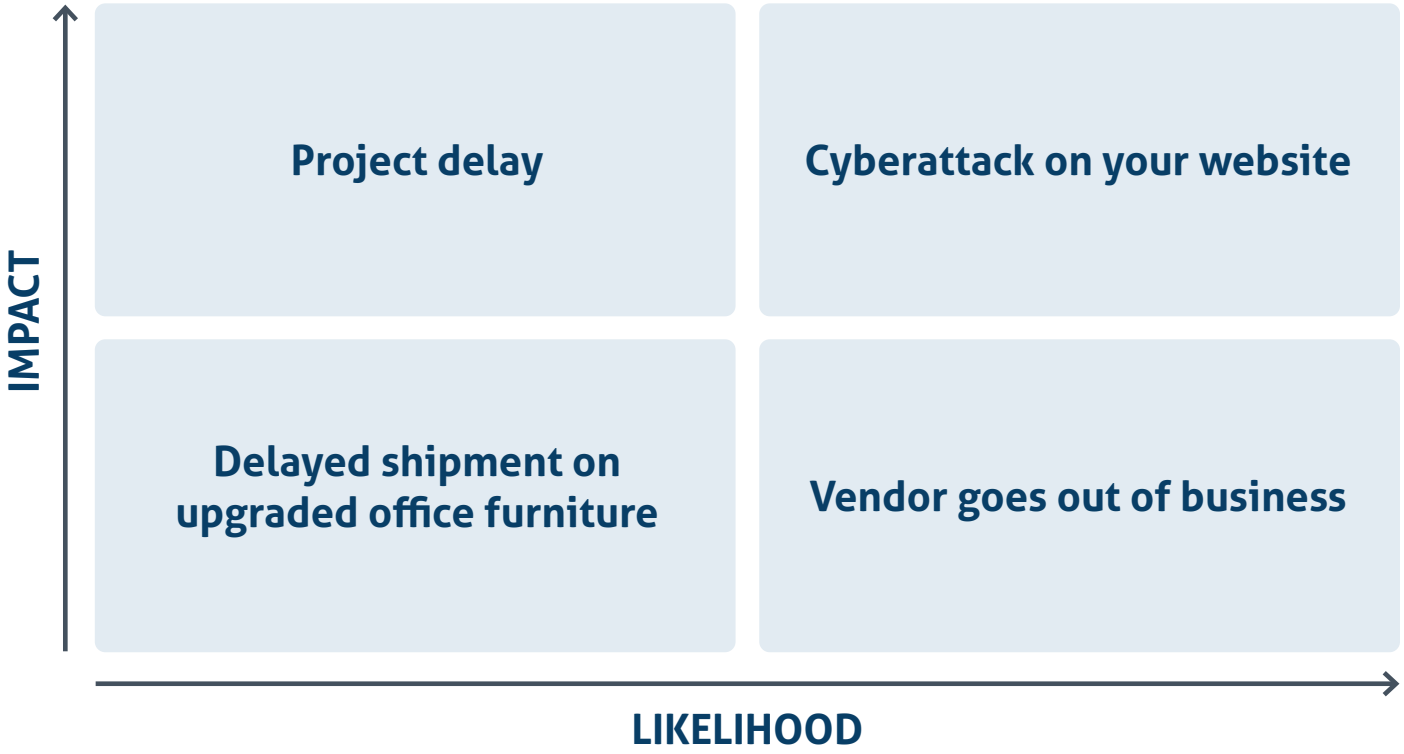
Risk Assessment

The goal of this exercise is to see where your organizations and its systems are most vulnerable to threats. While risks can come from anywhere — whether it be a flood, cyberattack or worldwide pandemic — disruption events can generally be narrowed down to four categories: loss of people, loss of building, loss of systems and data or loss of third-party services.

Use the space below to list any events you can think of that fall under these categories.

Prioritizing Risks

It's important to prioritize risks in addition to identifying them. This will help you decide where to allocate the most planning resources. It may be useful to create an impact and likelihood chart as seen below. We've filled in a few example events to get you started:



Business Impact Analysis

A well-formulated BIA should clearly identify how a particular event could affect your business.

Use the template below to create a BIA for one of the events your business wants to prepare for. Then repeat this process for each type of event you want to uniquely prepare for.

Disruption event type (such as project delay, cyberattack or an inaccessible office):

Types of losses from disruption (financial, productivity or reputation):

Level of losses (dollars or hours lost, whether reputation impact is light, severe or moderate):

Recovery point objective (If applicable, a tolerance threshold for how recent your backups need to be in case of a disruption.):

Recovery time objective (If applicable, a tolerance threshold for how long disruption can take place before business is impacted.):

Disaster Recovery Plan

How will you recover if a system goes down? Consider your geographic location, the nature of your business and any legal or regulatory frameworks:

It's important to repeat this process for each system, application and data store you want to recover.

Business Continuity Plan

List the steps to continue business if a process gets disrupted (such as payroll, hiring or accounts payable):

Process disrupted:

Nature of disruption (system, resources, personnel?):

Steps to resume:

It's important to repeat this process for each type of disruption you want to uniquely prepare for.

Crisis Management Response

An effective crisis management response requires finding the right team to make executive decisions in a crisis, as well as developing a communication strategy and detailed instructions on how to respond. Answer these questions for guidance on formulating a crisis management response.

Who is on your crisis management team?

Who will speak to the media?

Who will communicate with management, executives, board members and shareholders?

How will you communicate with your clients?

What will your organizational response be if members of the leadership team are incapacitated or unavailable?

How will you communicate with your staff if mobile phone, internet and other communications networks aren't operational?

You may want to create a checklist of key actions you want to take when a crisis occurs. List potential items on this checklist below. (Think about concerns such as safety, communication systems and so on.)

Testing Your Plan

With your business continuity strategy clearly outlined, you will want to test your plans to make sure they can be executed. Be sure to assess the effectiveness of your business continuity plans, disaster recovery plans and crisis management responses with testing that includes:

- Keeping reports of any external audits of your business continuity plans, disaster recovery plans and crisis management responses
- Regular review of testing plans, scenarios and results
- Proving issues identified in the gap analysis were resolved
- Specifying dates to test backup capabilities and verify that systems and data can be restored effectively