HOW TO ANALYZE

A Vendor's **Business Continuity** and **Disaster Recovery Plans**

venminder

How to Analyze

A Vendor's Business Continuity and Disaster Recovery Plans

Your organization probably dedicates a lot of thought, time and resources to its business continuity (BC) and disaster recovery (DR) planning and testing. Similarly, your third-party vendors should be just as committed to their plans and testing. When unplanned outages or business-impacting events occur, business continuity management ensures that essential operations, products and services are available fully or to a predetermined level of availability.

How do you confirm that your vendors have effective BC/DR plans? This eBook covers the main sections that you should be searching for in each plan and what to know about each of them.

Beginning with the vendor's business continuity plan (BCP), you'll want to make sure certain components are included and activities have been performed.

Make sure you review the following four areas as you analyze the plan:

1 Evidence of a formal, written plan addressing valid concerns

The plan should address various scenarios and how they affect people, facilities and processes.

2 The inclusion of the following 7 key components:

Ongoing Maintenance

There should be ample evidence that the business continuity plan is reviewed and modified, if needed, on a recurring basis. This might be annually, quarterly or bi-annually. The plan might need to be updated and documented after any significant organizational changes. Maybe the vendor has experienced changes to the staff or significant employees have joined or left the company. Perhaps they've implemented new processes, introduced new products or have simply made an overall change in business operations. Any of these factors should prompt an update to their business continuity plan.

Identified Teams or an Individual

The BCP should be created and maintained by a dedicated person or team.

Personnel Recovery to Normal Operations

The plan should identify a physical space or process that allows employees to continue working if the primary office location is unavailable. This can be things like work from home/remote work options or workload shifts to operational offices.

Alternate Location Type

Here's what you may find:

Cold Location
An empty building that isn't stocked with required items like desks, copiers, critical documents, etc. This location would need significant preparation to be able to occupy and utilize.

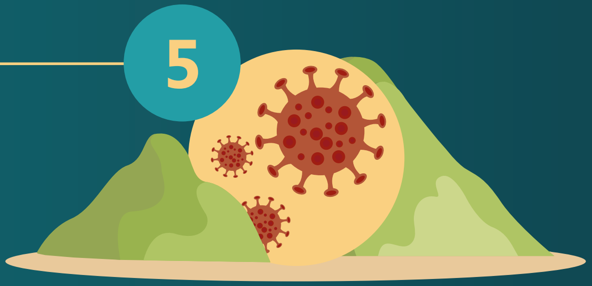
Warm Location
A building that has most or all the required items onsite. It can be ready to use with minimal preparation.

Hot Location
This building has all necessary items and maintained inventory. Employees can use a hot location at any moment without any preparation.

Important Note: An alternate location is NOT the same as failover data center location in which additional IT hardware/servers and networking equipment are maintained.

Plans for Pandemic Related Events

The plan should provide details on activities related to mass illness, significant absenteeism or the inability to travel or occupy locations because of health risks.



Board of Directors and/or Senior Management Involvement

The board of directors and/or senior management should be actively involved in the creation, reviews and approvals of the business continuity plan on a reoccurring basis.

Documented Client Notifications Procedures

After a business impacting event has occurred and the BCP has been activated, it's important that your organization is notified to ensure that your expectations and needs will be met. The vendor's plan should include a documented client notification process via email, phone call or automated alert which states the details of the event and whether service levels have been impacted.

3 Proof of testing

In addition to the details of the plan, ensure that the vendor is actively testing it. Unless the business continuity plan is tested, you won't know for sure that it's effective. You should expect to review the frequency, type and evidence of testing:

Frequency

Ensure the business continuity plan has been tested within the last 18 months.

Type

Not all types of testing are equal. Here's a breakdown of three common types:

TABLETOP

A verbal walkthrough of the plan when given a hypothetical event. It usually involves inactive role playing around the table.

SIMULATED

It requires a little more activity. Individuals will usually engage in active role-playing and perform certain BC activities or functions. However, the activities are performed in a way that doesn't affect normal operations.

FUNCTIONAL

Requires the most activity, as these are full enactments of what to do during and after an event.

BCP Testing Evidence

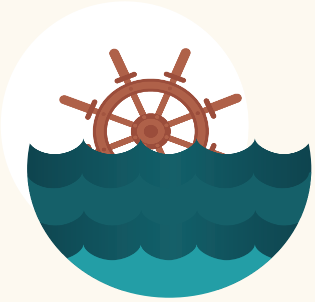
You'll want to make sure that the testing was completed successfully or that any identified issues have been addressed or are in the process of being addressed. If any areas didn't work as expected, ensure that the vendor is following through to fix them.

4 Evidence that a business impact analysis has been regularly performed, reviewed and updated regularly

A business impact analysis (BIA) essentially determines the vendor's criticality. In other words, how would a disaster, accident or emergency potentially affect and interrupt critical business operations? An important part of reviewing a vendor's BIA is confirming the existence and documentation of recovery time objectives (RTOs) and recovery point objectives (RPOs). It's important to ensure that RTOs and RPOs are established for the applicable service and that they meet your organization's needs.

Here's a brief explanation of these two terms:

- **Recovery time objective** refers to the targeted duration of time in which a business process must be restored after an event. This duration of time is predetermined and calculated to avoid unacceptable consequences that are associated with a break in business continuity.



- **Recovery point objective** is the maximum amount of data loss that's acceptable in a worst-case scenario, in which the vendor can still operate.

While business continuity plans have more emphasis on resiliency over time, disaster recovery plans (DRPs) focus on the immediate strategy of what to do when an event occurs. As with a business continuity plan, you'll want to make sure that the vendor's disaster recovery plan incorporates certain elements. When reviewing the plan, you'll want to verify that the vendor has accounted for these five things:

1

Evidence of a formal, written plan addressing valid concerns

The plan should address concerns like IT hardware, servers, data centers and networking equipment.

2 The identification of the following 3 areas:

Recovery Locations, Data Center or Server Rooms

Make sure the plan documents the location details around the primary data center and recovery sites that are used to store, process or provide data services.

Disaster Recovery Site Configuration

This will include cold, warm and hot locations:

A cold location is an empty building or data center that doesn't have servers, network hardware or backup data. Significant preparation is needed to use a cold location.

A warm location only requires minimum preparation to use because it contains the necessary servers, network hardware and backup data on site.

A hot location is fully prepared with the required servers, network hardware and back up data. It should be ready to use at any moment either by itself or in tandem with the primary site.

Geographic Diversity

It's important to verify that the vendor's primary and recovery sites are located at such a distance that a single event is unlikely to impact both.

3

Evidence that the plan has been tested

The plan should have been successfully tested within the last 18 months. The plan should also identify any issues that were found and whether they have been addressed or are currently being addressed. The following testing methods should be included:

TABLETOP

A verbal walkthrough of the plan given a theoretical event. This usually involves inactive role playing.

SIMULATED

An exercise where certain DR activities or functions are carried out in a way that doesn't impact or change normal operations. Active role playing may be involved.

FUNCTIONAL

A full test/failover where production is moved.

DRP testing evidence

Evidence that testing was completed successfully or that identified issues either have been or are currently being addressed.

4

Backup procedures are in place

These are critical in a disaster recovery plan as they help validate whether data is safe and accessible during and after an event. Make sure the following backups are performed and documented:

On-site Backups

Performed and stored in the same location as the data that's backed up, such as an on-site safe.

Off-site Backups

Performed and removed to be stored at a separate physical location.

Replicated to Alternate Location

Backup data is copied over a network link to another physical location.

Monitored Alerts

Provide evidence that backup jobs/logs are reviewed or that alerts are generated for backups that were terminated in an abnormal or failed state.

Encryption

Backup data should be confirmed, along with evidence that the data will be transferred over a network link to an alternate physical location.

5 Backup procedures testing

Without testing of the backup procedures, you won't know whether they work. The DRP should include evidence that backup data is tested or restored on a periodic basis, at least annually. This confirms that backups are accessible if they're needed.

Conclusion

A good vendor risk management program should always include business continuity and disaster recovery reviews. This provides a strategic advantage where organizations can better avoid risky scenarios that negatively affect its operations and reputation. Remember that business continuity management should be a priority not only for your vendor's business strategy, but also for your own organization.

Download a free sample Business Continuity and Disaster Recovery Assessment see how Venminder can help reduce your third-party risk management workload.

Download Now

venminder

Manage Vendors. Mitigate Risk. **Reduce Workload.**

+1 (888) 836-6463 | venminder.com

About Venminder

Venminder is an industry recognized leader of third-party risk management solutions. Dedicated to third-party risk, the company is the go-to partner for software, high-quality assessments on vendor controls, certified subject-matter expertise and education.

Venminder's platform provides a centralized location to execute a third-party risk management program. It enables users to store documentation, onboard a vendor, track contracts, manage SLAs, send and manage questionnaires, manage due diligence and oversight, complete risk assessments, create workflows, run reporting and more.

Assessments performed by Venminder's qualified experts, including CISSPs, CPAs, financial risk analysts, paralegals and more, are readily available in an online exchange library. The assessments enable customers to identify possible risks and understand areas of strength on their vendors' information security and privacy standards, SOC reports, financial viability, business continuity/disaster recovery preparedness, contractual standards, regulatory compliance and more.