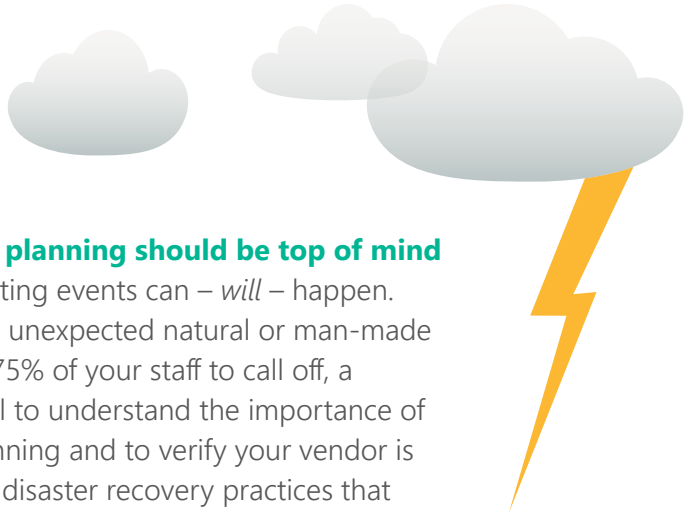
Are You Reviewing Your Vendor's BCP and Disaster Recovery?

venminder



Business continuity and disaster recovery planning should be top of mind all of the time. Like it or not, business impacting events can – *will* – happen. Your organization isn't immune. These can be unexpected natural or man-made disasters such as a hurricane, the flu causing 75% of your staff to call off, a power outage, flood, etc. Therefore, it's critical to understand the importance of business continuity and disaster recovery planning and to verify your vendor is implementing strong business continuity and disaster recovery practices that align with your own plans.

In this eBook, you'll learn more regarding what business continuity and disaster recovery are, the importance, what can go wrong if both aren't done properly and how to thoroughly analyze your vendor's business continuity plan (BCP) and disaster recovery plan (DRP).

Why Is Reviewing a Vendor's BCP and DRP Important?

First and foremost, before digging further into the bones of BCPs and DRPs, let's understand why reviewing a vendor's BCP and DRP is so important. What can go awry if you don't? A vendor with a faulty BCP or DRP can be a recipe for disaster for these four reasons:

- **Unprepared Vendor:** This could lead to the vendor flying by the seat of their pants in order to resume uptime. Not a comforting feeling when you're relying on them for your own operations to resume.
- **Operational Delays:** This could mean your organization's operations are interfered with for longer than anticipated or longer than the downtime allotted for in your own BCP/DRP.
- **Data Loss:** The vendor may lose, and not be able to recover, some of your organization and customer data.
- **Reputational Hit:** Your organization's reputation could be at risk due to the vendor's failure to implement comprehensive, well-developed BCPs and DRPs. Your customers, and even the media, will think it's your organization who isn't prepared! They can't see behind the scenes.

Business Continuity Plan

What Is It?

Business continuity planning helps an organization ensure that their critical operations, products and services are always delivered in full or at a predetermined level of availability. These expectations tend to be outlined in a service level agreement (SLA) with the vendor. The BCP provides an overview of the precautions in place and the testing that has been done to ensure measures have been established to prevent the cease of operations in case of a business impacting event.

What Does a BCP Include?

A BCP should address the following three areas:

- Planning for loss of personnel, facilities or services
- Planning with public entities (emergency services, local and state disaster relief agencies)
- Communicating with significant vendors, clients, employees and the media

How to Properly Analyze a BCP

Are you performing these 10 critical steps?

1. **Verify the vendor has a formal BCP.** Determine whether a formal, written plan exists, meets your organization's needs and covers critical components that are needed to ensure operations continue. If the vendor becomes unavailable, will your services operate normally?

2. **Review the vendor's strategy for addressing personnel loss –** aka their succession plan. Look for cross-training, job rotation, staffing agencies, etc. as mitigations. Social unrest may occur.

3. **Determine if the BCP contains plans for pandemic contingencies or mass absenteeism** following Center for Disease Control guidelines. How will the vendor continue operations without key personnel?

4. **Check their relocation plans.** Confirm they're acceptable and verify the vendor has a secondary office facility or remote work capabilities. This includes things like assets, equipment, building relocations, remote access strategy, contract third party office space and more. Ask yourself questions like can other locations handle the load, is their office recovery space within another building and is the secondary location always ready?

5. **Review their breach/disruption notification policy** to verify a clear communication plan is in place, it's adequate and aligns with the information security language that's in the contract between your organization and the vendor. *This step is very important* as it's confirming the timing of when the vendor will notify your organization of a breach or disruption, so you want to make sure it's acceptable and meets any requirements you have, including regulatory requirements.

6. **Review the vendor's Business Impact Analysis (BIA) within the BCP and that it matches your expectations.** This includes the following:

- **Recovery Time Objectives (RTO):** RTO help identify the targeted duration of time in which the vendor must restore a business process, post-disruption, to avoid unacceptable consequences associated with business continuity.
- **Recovery Point Objectives (RPO):** RPO help identify how much data may be lost if data needs to be recovered. Typically, this matches with your backup or replication frequency. It's critical to review and understand RPO because it will become very important if a computer, system or network goes down.
- **Maximum Tolerable Downtime (MTD):** MTDs specify the maximum period of time that the vendor can be down before their survival is at risk.

How much data may be lost and how long will normal operations be impacted? This is what you're learning when reviewing RTO and RPO. Some vendors will have different objectives for different services and client tiers. How does this relate to your contracted SLA?

7. **Understand the vendor's testing procedures.** Ensure the testing is at least annual and ask to see the actual or redacted test results. Any testing results showing room for growth should be followed up on.

8. **Analyze the frequency of ongoing maintenance of the plan.** The BCP should be reviewed regularly as part of the vendor's routine policy maintenance but should also be updated when a significant change occurs in the vendor's organization.

9. **Have a qualified subject matter expert (SME) write up the analysis.** This should be an experienced IT professional or someone with a related credential.

10. **Reach out to the vendor to discuss any findings and next steps.** Keep the analysis handy and reference as needed.

Disaster Recovery Plan

What Is It?

Disaster recovery planning keeps your organization informed regarding what the appropriate response to a business impacting event should be based on the event type that occurred. Disaster recovery planning is a subset of business continuity planning. A DRP involves processes and procedures for an organization to follow immediately, as soon as a business impacting incident occurs, until normal operations are resumed.

What Does a DRP Include?

A DRP should address the following five areas:

- Procedures for disaster recovery personnel
- Determining what constitutes as a disaster incident
- Implementing the DRP in accordance with the BCP
- Coordinating with public entities as needed
- Resumption of normal operations

How to Properly Analyze a DRP

Are you performing these 11 critical steps?

1. **Verify the vendor has a disaster recovery plan in place that is readily available to staff in the event of a disaster and addresses data loss and system availability.** How much data may be lost and how quickly availability is restored should be represented by RTO and RPO.

2. **Check whether criteria is defined and in place for declaring a disaster.** Without defined internal communication and an incident management program, employees may not know when to formally declare a disaster, attempting to fix the business impacting event instead of communicating the issue to key stakeholders.

3. **Verify the plans cover availability and potential loss of equipment, data and the data center/server room.** Does their plan fit your security and availability requirements? Look at how data is stored, the location and status of the recovery information system.

4. **Check if a secondary data center is readily available** in the event of a disaster and ensure it's sufficiently geographically separated so that a regional impacting event won't affect the vendor's production and recovery sites simultaneously.

5. **Review the configuration of the vendor's data center recovery locations** to assess the adequacy of recovery capacity to meet your business needs.

6. **Ensure that a clear communication plan is in place and verify their client notification process meets your requirements.** When issues occur, communication can save a relationship. Verify that the vendor's notification timeline meets any requirements you have, including regulatory requirements.

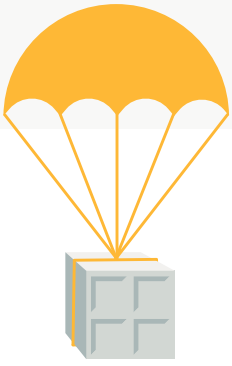
7. **Review critical IT functions outsourced to a third party** and ensure communication plans exist with subcontractors (aka your fourth parties).

8. **Understand the vendor's testing procedures.** Ensure the testing is at least annual and ask to see the actual or redacted test results. Any testing results showing room for growth should be followed up on.

9. **Analyze the frequency of ongoing maintenance of the DRP.** Plans should be reviewed annually and after any significant organization changes as part of the vendor's routine policy maintenance.

10. **Have a qualified SME write up the analysis.** This should be an experienced IT professional or someone with a related credential.

11. **Reach out to the vendor to discuss any findings and next steps.** Keep the analysis handy and reference as needed.



The Guidance

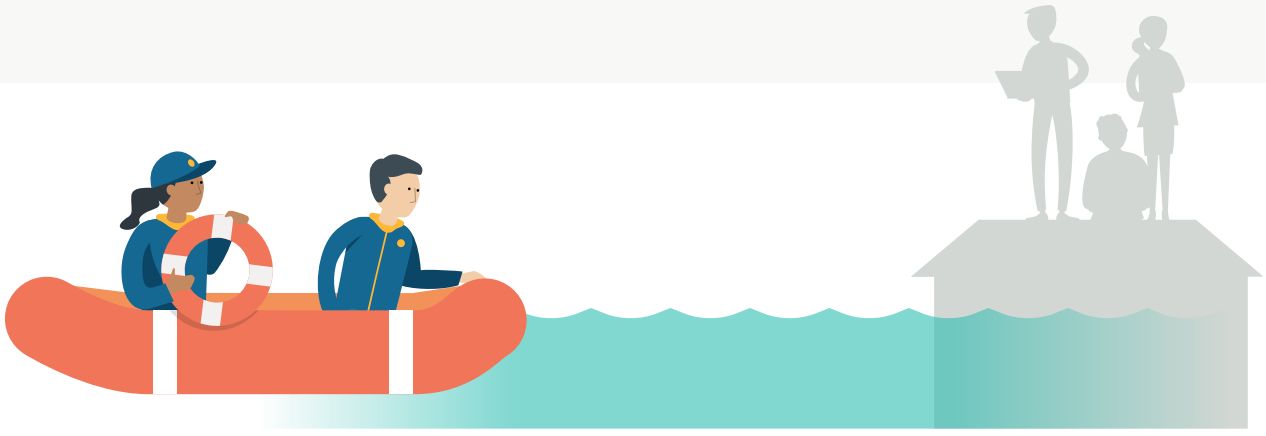
Looking for more resources to help you understand BCPs and DRPs a little further? Here's some of the guidance we encourage you to review to deepen your understanding and help you determine what examiners are looking for.

- **FFIEC Examination Handbook on Business Continuity Planning**
- **FFIEC Appendix J**
- **FINRA Rule 4370**
- **FDIC FILs** 62-2017, 6-2008, 49-2006, 25-2006, 84-2002

4 BCP/DRP Best Practices to Remember

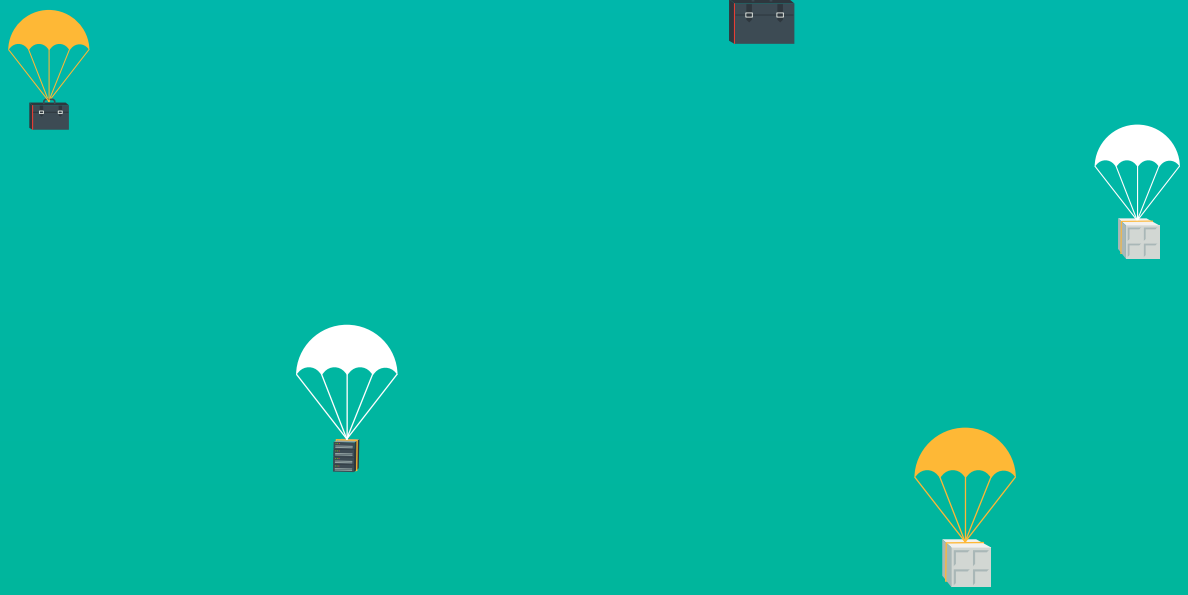
- Establish a process to follow when a vendor experiences a business impacting event.
- Contractually commit the vendor to test their plans at least annually.
- Set clear expectations and notification requirements with the vendor.
- Document your vendor BCP/DRP reviews and address the findings with the vendor – regulators expect this.

Implementing practices around vendor BCP and DRP reviews isn't necessarily difficult, but it does require a lot of work. However, the hard work pays off by protecting your organization, operations, customers and reputation.



Download free work product samples and see how Venminder can help reduce your vendor management workload.

Download Now



venminder

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

(270) 506-5140 | venminder.com

About Venminder

Venminder is a leading third party risk management provider dedicated to helping the financial services industry mitigate vendor risk.

Venminder's team of due diligence experts offer a suite of services that can significantly reduce the workload by addressing the tactical challenges of vendor management tasks. Venminder's vendor management software can guide a user through critical processes such as risk assessments, due diligence requirements and task management.