

Rules to Receive CPE Credit

By attending today's session, you are eligible to receive 1 CPE Credit per the following guidelines:

In order to receive this credit, the following items MUST be completed:

- ✓ Each person wishing to receive CPE Credit must log into the session individually with their credentials
- ✓ You MUST answer ALL of the polling questions throughout the presentation
- ✓ You MUST be in attendance for the entire live session
- ✓ You MUST complete the follow-up survey regarding the session





Understanding Vendor Business Continuity, Disaster Recovery, and Pandemic Plans

PRESENTED BY

Lisa-Mae Hill



Information Security Operations Director
Venminder
lisa-mae.hill@venminder.com

August 23, 2022

Session Agenda

1

What business continuity, disaster recovery, and pandemic plans are and why they're important

2

How to review your vendor's plans

3

What auditors and regulators expect you to know

4

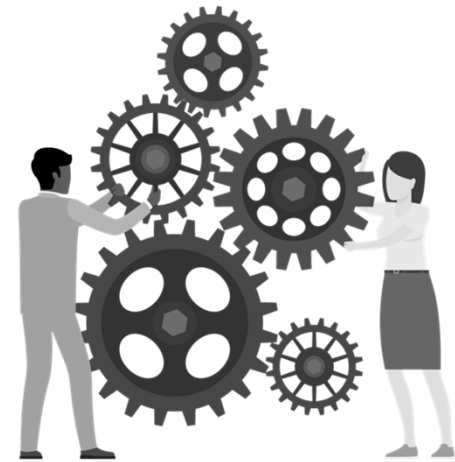
Best practices for vendor business continuity management

Business Continuity Management (BCM)

- BCM is an umbrella term that encompasses business continuity, disaster recovery, and pandemic planning.
- A vendor's BCM program should align with its strategic goals and objectives. Management should consider a vendor's role within and impact on the overall industry when it develops a BCM program.
- Requires management to have processes in place to oversee and implement resilience, continuity, and response capabilities to safeguard employees, customers, products, and services.
- Resilience incorporates proactive measures to mitigate disruptive events and evaluate an organization's recovery capabilities.

What Is Business Continuity and Disaster Recovery?

- **Business continuity** allows you to ensure that key operations, products, and services continue to be delivered either in full or at a predetermined, and accepted, level of availability.
- **Disaster recovery** is a subset of business continuity and outlines the process and procedures to follow at the immediate onset of an incident up to and including the resumption of normal operations.
- You do this for your own organization, but you should also be aware of what your vendor does.



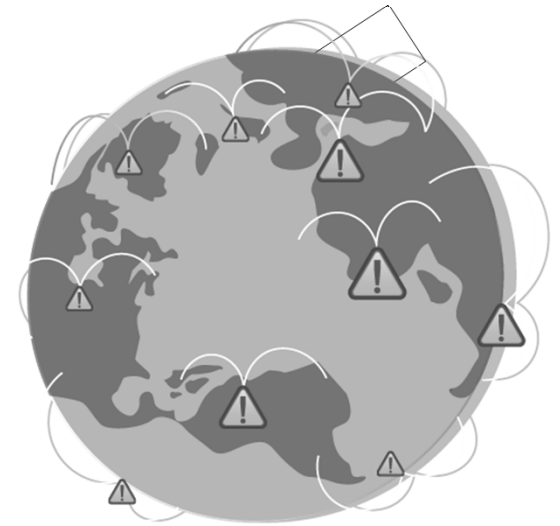
Business Continuity / Disaster Recovery Terminology

- **Business Impact Analysis (BIA)** – Used to determine the impact on the organization of the loss of a specific business function within a line of business
- **Recovery Time Objective (RTO)** – Help identify the targeted duration of time which the vendor must restore a business process, post-disruption, to avoid unacceptable consequences associated with business continuity
- **Recovery Point Objective (RPO)** – The interval of time that would pass during a disruption before the quantity of data lost during that period exceeds a predetermined maximum allowable threshold or “tolerance”
- **Maximum Tolerable Downtime (MTD)** – Specify the maximum period of time that the vendor can be down before the disruption in services could cause a significant or material loss



What Is Pandemic Planning?

- Preparing for a pandemic event by planning, exercising, revising, and translating actions as part of a response
- A **pandemic plan** is an active document which lists the strategies, procedures, preventative measures, as well as any corresponding implementation guidelines an organization will take should a global health crisis occur
- Your vendor's pandemic plan will tell you how they plan to continue operating and providing business services during unprecedented events



Monitoring Vendor Pandemic Planning

- Reviewing vendor pandemic plans and cybersecurity measures
- Reviewing your own BIA
- Referring to regulatory guidance
- Communicating your plans and expectations to your vendors
- Testing your plan and your vendor's plan frequently



Reviewing Vendor Pandemic Planning

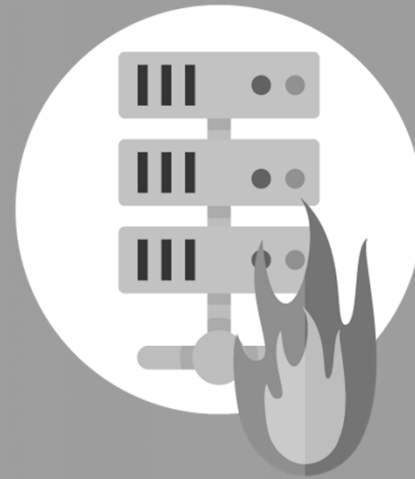
What should you look for in a pandemic plan?

1. Preventative Program(s)
2. Documented Strategies
3. Comprehensive Framework of Facilities, Systems and Procedures
4. Testing Programs and Results of Tests
5. Oversight Programs



Real-Life Scenarios Will Happen

It's Just A Matter of Time



Poll Question

Do you feel your pandemic plans are adequate and prepare you for pandemic scenarios?

- a. Yes – we are in good shape
- b. No – we are not prepared
- c. Maybe – it seems we are somewhat prepared
- d. Not sure

The BCM Cycle

1. **Oversee and implement** resilience, continuity, and response capabilities
2. **Align BCM elements** with strategic goals and objectives
3. **Develop a BIA** to identify critical functions, analyze interdependencies, and assess impacts
4. **Conduct a risk assessment** to identify risks and evaluate the likelihood and impact of disruptions
5. **Develop effective strategies** to meet resilience and recovery objectives
6. **Establish a business continuity plan** that includes incident response, disaster recovery, and crisis management
7. **Implement a business continuity training program** for personnel and other stakeholders
8. **Conduct exercises and test** to verify that procedures support established objectives
9. **Review and update the business continuity program** to reflect the current environment
10. **Monitor and report** business continuity resilience activities

Vendor Board/Executive Leadership Oversight

- The board/executive leadership govern business continuity, disaster recovery, and pandemic planning through defining responsibilities and accountability and by allocating adequate resources to business continuity.
- Ensure your vendor's plans include board/executive leadership oversight.
- **Three major responsibilities of the board/executive leadership include:**
 - Aligning business continuity, disaster recovery, and pandemic planning with the organization's business strategy and risk appetite
 - Understanding the risks and adopting policies and plans to manage events
 - Reviewing the operating results and performance through management reporting, testing, and auditing



Vendor Senior Management Oversight

- Ensure senior management is engaged in business continuity, disaster recovery, and pandemic planning.
- **The major responsibilities of senior management include:**
 - Designing and implementing a business continuity exercise strategy
 - Establishing measurable goals against which business continuity performance is assessed, such as levels of preparedness and resilience targets
 - Validating that personnel understand their business continuity roles and responsibilities
 - Confirming that exercises, tests, and training are comprehensive and consistent with the organization's strategy and resolving identified weaknesses
 - Updating strategies and plans to reflect the current business conditions and operating environment



Audit and Examinations: What the Regulators Expect

The board/executive leadership and senior management should engage internal audit or independent personnel to review and validate the design and operating effectiveness of the BCM program.

- **Examiners will want:**
 - An analysis and review of your third party's business continuity, disaster recovery, and pandemic plans
 - Documentation available
- **Examiners will review for the following:**
 - Alignment of BCM elements with the vendor's strategic goals and objectives
 - Board oversight
 - Management assignment of BCM-related responsibilities
 - Development of BCM strategies



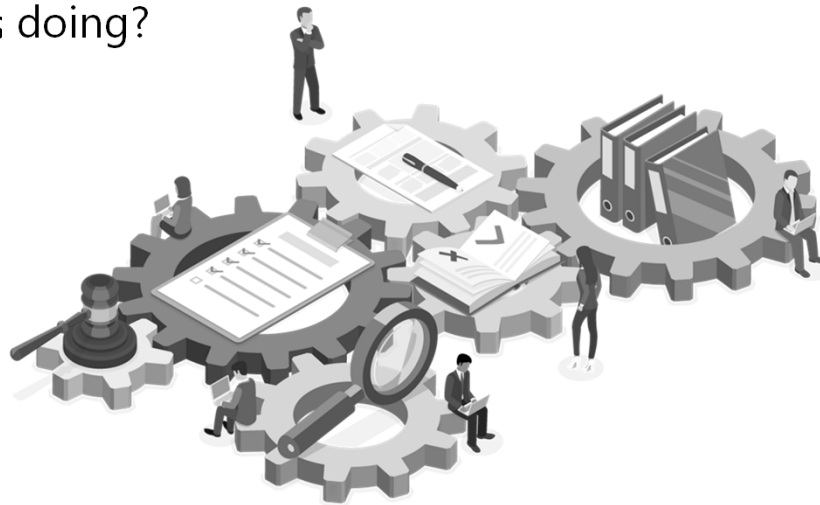
Poll Question

Do you review your critical third parties' business continuity, disaster recovery, and pandemic plans on a regular recurring basis?

- a. Yes
- b. No
- c. Not sure
- d. Not applicable

Vendor Risk Management and BCM

- BCM is risk-based!
- BCM requires a business impact analysis and focuses on operational risk factors.
- BCM involves managing the possibility of an event that jeopardizes critical systems.
- What are your vendors doing?



What Is a Business Impact Analysis (BIA)?

An analysis to determine if your organization can operate effectively while the vendor is unavailable.

- Management should develop a BIA
- Review if there is updated regulatory guidance or when significant change occurs within your organization or the vendors
- It's all about the risk

Ask yourself:

1. Would a sudden loss of this vendor cause a material disruption to my organization?
2. Would that sudden loss of this vendor impact our customers?
3. Would the time to recover operations exceed 24 hours or would there be a negative impact to your organization?



venminder

Why It's Important

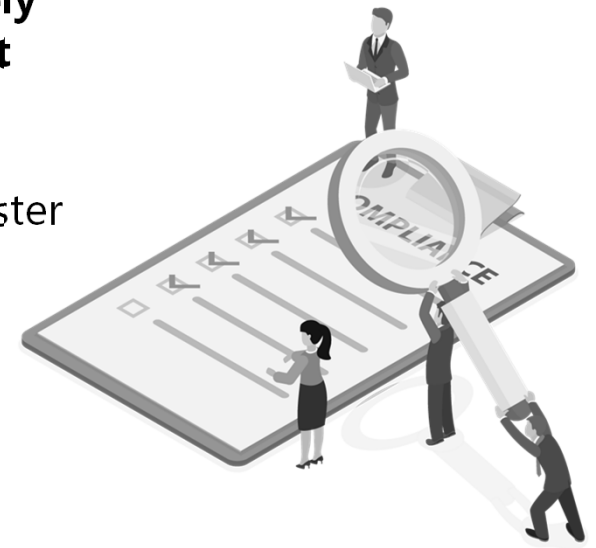
Would your third party survive in the face of disruption?

If your BIA shows that your organization can't operate effectively while a vendor is unavailable, your third-party risk management program should include:

- Thoroughly evaluating the vendor's business continuity, disaster recovery, and pandemic plans
- Understand the procedures they have in place to handle a business impacting event

This allows you to:

- Be aware of possible downtimes and what could affect your operations or reputation
- Plan accordingly with your own BC/DR plans



What the BIA Should Include

- Must include critical business functions, including support activities systems, and interrelationships may be analyzed in several ways
- Workflows, interviews, organizational charts, network diagrams/topologies, data flow diagrams, succession plans, or delegations of authority for key personnel may help management identify business processes and hierarchies
- Management must conduct an interdependency analysis which should identify single points of failure in close geographic proximity



Reviewing the Vendor's Business Continuity Plans

Review these key areas of those plans to provide assurance that your vendor is prepared for a disruption:

- Testing procedures
- Copies of the plan are held off-site in secure locations and available
- Plan is reviewed, tested, and updated regularly
- Results of any recent tests, and if the test didn't go well, the vendor's remediation plans
- Senior management and board approval
- SLAs and contractual obligations
- Failover and backup locations
- Personnel loss and planning
- Relocations plans
- Remote access availability
- Facility loss contingencies
- Pandemic contingencies
- Breach/disruption notification procedures



Your vendor's business continuity plans, and their preparedness, should meet or exceed your own plans.

Reviewing the Vendor's Disaster Recovery Plans

Look at these key areas when reviewing the vendor's disaster recovery plans:

- Dedicated team and individuals
- Testing, results of recent tests, and updates
- Notification process
- Pandemic plan
- Backup procedures
- Personnel recovery to normal operations
- Business impact analysis
- Senior management/board approval and involvement



Reviewing the Vendor's Pandemic Plans

Look at these key areas when reviewing the vendor's pandemic plan:

- **Preventative programs**
 - Communicate with critical vendors, monitor outbreaks, educate employees
- **Document strategies**
 - Consistent with the CDC
- **Framework of facilities, systems, and procedures**
 - How to sustain operations
- **Test programs**
 - Confirm the plan is effective
- **Oversight programs**
 - Reviews and updates



Poll Question

Do you ask where your vendor's BCM program reports to in their organization?

- a. Yes
- b. No
- c. Not sure
- d. Not applicable

Vendor BCM Stresses Resilience

Determine you vendor's resiliency by asking for the following:

- Evidence of physical resilience
- SOC Type II reports and independent audits to determine cyber resilience
- Data backup and replication strategies being used
- A pandemic plan covering the loss of personnel
- Your vendor's change management policy and program
- Event management plans
- Facilities and Infrastructure
- Data Center Recovery Alternatives
- Branch Relocation
- Electrical power redundancy
- Telecommunications redundancy plans



Ensure Vendors Exercise and Test



Full-Scale Exercise

- Transfer of live production environment to another data center



Limited-Scale Exercise

- Mirroring production environment to another data center and testing functionality, but not transferring traffic



Tabletop Exercises

- Walk through the steps to recover from an impacting event with key personnel, without testing systems



Tests

- Industry exercises and resilience
- Third-party service provider testing
- Post exercise and post test actions



Protection Inside Vendor Contracts

Protect yourself with your contract.

Within your contracts, ensure that they provide:

- Accessibility to the vendor's BCM, Policies and Procedures (P&P), and Program
- Independent testing requirements
- Frequency and availability of test results
- Recovery times
- Backup responsibilities
- Cyber resilience
- Management of third-party/outsourced business continuity
- Breach/disruption notification



Best Practices to Takeaway



- ✓ Assess risk early and be thorough
- ✓ Have clear guidelines on what must be done at each stage of the relationship (and be sure pandemic plans are being considered)
- ✓ Contractually commit the vendor to test
- ✓ Record anticipated results, assess any vulnerabilities, thoroughly document
- ✓ Ensure plans include contingencies or mass absenteeism following disease control guidelines
- ✓ Check that relocation plans are clear
- ✓ Real-life problems do happen – we're in it now
- ✓ Clear expectations and notification requirements

Thank You




venminder

Also Join Us At Our Upcoming Webinars:



(Today) AUGUST 23, 2022, at 2pm ET

Deep Dive Into Vendor Business Continuity, Disaster Recovery and Pandemic Plans Webinar

AUGUST 25, 2022

How to Determine Which Vendors Are Critical to Your Credit Union

SEPTEMBER 6, 2022

What the Board & Senior Leadership Need to Know About Third-Party Risk Management Webinar

[Click here](#) to view our Webinars Page.



Questions and Answers

Post a Question:

www.thirdpartythinktank.com



Email Us:

lisa-mae.hill@venminder.com

Follow Us:

@venminder

