Beyond the Plan: Using Third-Party Risk and Performance Monitoring to Improve Operational Resilience

September 27, 2023

PRESENTED BY

Hilary Jewhurst

Head of Third-Party Risk Education & Advocacy
Venminder

venminder

Session Agenda

1. The basics of business continuity plans
2. Risk and Performance monitoring, and the connection to successful business continuity planning
3. Risk monitoring
4. Performance monitoring
5. Issue management

venminder

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.

venminder

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.

venminder

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.

venminder

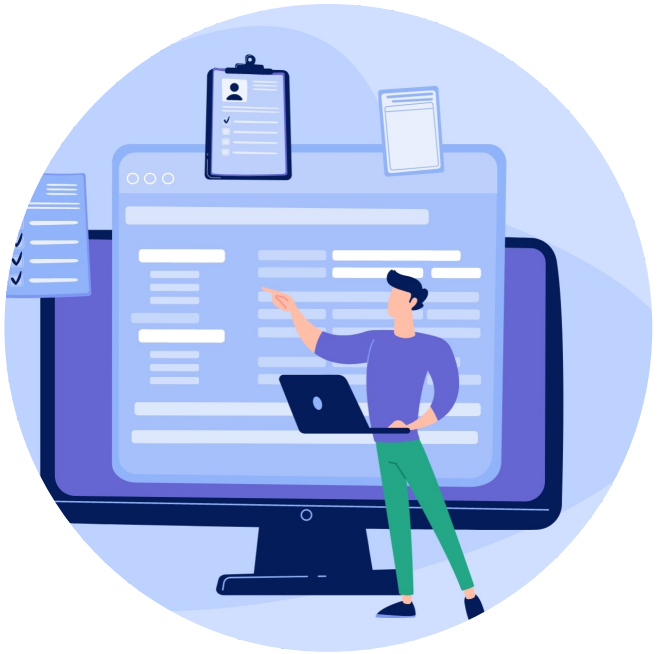
Why Business Continuity Management (BCM) Is Important

- Direct impact on availability
- BCM allows for you and your vendors to proactively plan for disasters and business interruptions
- Allows you to provide assurance to your customers that your product/service will always be available
- Protects your organization from data loss

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

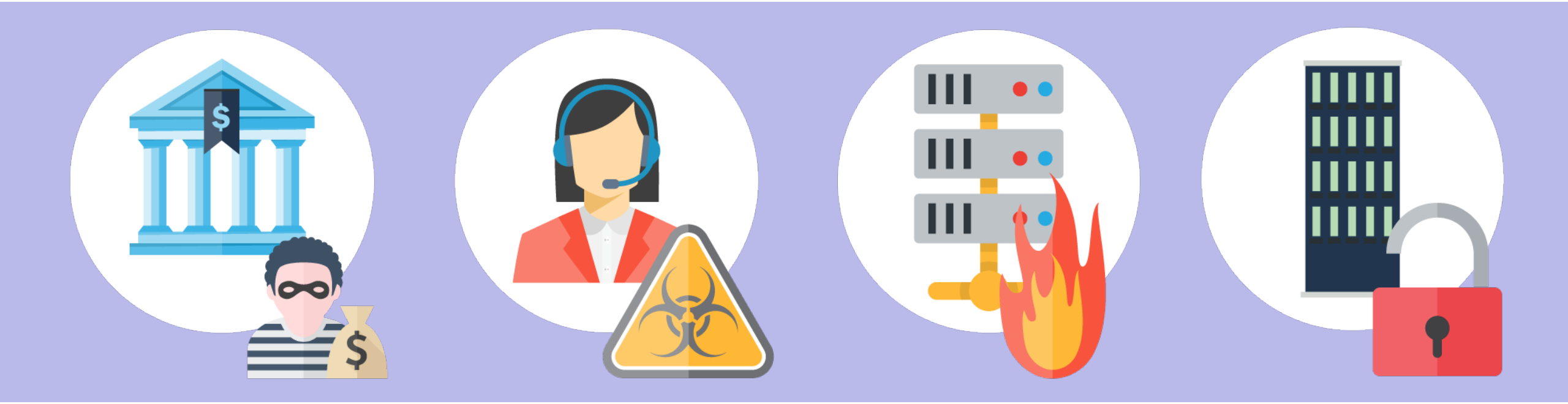
Examiners will review for the following:

- Alignment of BCM elements with the vendor's strategic goals and objectives
- Board oversight
- Management assignment of BCM-related responsibilities
- Development of BCM strategies

venminder

Real-Life Scenarios Will Happen

IT'S JUST A MATTER OF TIME



The Importance of Reviewing BCP Plans

A business continuity plan (BCP) for vendors is an essential aspect of an organization's overall strategy. It helps to guarantee that your vendors will continue to provide products and services to your organization, even during a business-disrupting event, at an agreed-upon level of availability. This is typically outlined in the vendor contract through a detailed service level agreement (SLA).

Your vendor's business continuity plan should initially be reviewed during the vendor vetting and selection stage of the relationship, as well as on an annual basis through your ongoing monitoring duties. It's important to continually monitor your vendor after you've selected and contracted with them to keep informed of any concerning changes.

venminder

Reviewing the BCP – Red Flags

- **BCPs that are limited to IT disaster recovery information.** Some vendors do not differentiate between business continuity (e.g., people, processes, and facilities) and IT disaster recovery (e.g., information systems, data, and networks).

- **BCPs that haven't been updated or tested within the last 12 months or within the time range defined by the vendor in their plans.** Regular testing of your vendor's BCP will ensure that it will operate as expected when a disaster strikes. It should also be updated to reflect any changes within the organization.

venminder

Reviewing the BCP – Red Flags

CONTINUED

- **BCPs that don't address products/services that are applicable to your organization.** Your vendor may have multiple BCPs for different product lines, so it's important that the plans you review are written specifically for the products/services used by your organization.

- **RTOs and RPOs aren't defined or don't align with your recovery needs.** If RTOs and RPOs are outside of your needed time frame to provide products/services to your customers, then additional measures may be needed. Understanding what level of service you should expect after a business-impacting event at your vendor will ensure you're prepared to handle any decline in service, availability, or functionality.

Keep in mind that any of the following are also cause for concern:

- Applicable RTOs weren't met or adjusted.
- Applicable RPOs weren't met or adjusted.
- There are no remediation plans established for the issues identified.

Note: *It's important to understand that RTO refers to an "established level of service" and doesn't necessarily mean a recovery to full operations.*

venminder

The Connection Between Successful BC/DR Plans and Risk and Performance Monitoring

Business Continuity/Disaster Recovery (BC/DR) plans are designed to ensure that a vendor can continue operating smoothly during or immediately after a business-interrupting event. To ensure the successful continuation of operations, the vendor must meet all necessary baseline requirements in the first place.

- The vendor’s ability to execute the BC/DR plan could be at risk if the vendor has any new, evolving, or unmanaged risks.
- Business interrupting events can arise from unmanaged risks.
- Organizations need to ensure that vendors meet the expected service level requirements. If a vendor's performance is already declining or substandard, it could lead to even bigger problems in the event of a business interruption.

venminder

CorEX-Servpro – A Case Study

CorEx-Servpro is a (fictional) organization responsible for providing core processing services to its customers.

A core processing system is a behind-the-scenes mechanism that handles banking transactions within a bank's different branches. It encompasses deposit, loan, and credit processing functions and is a critical service for a banking organization.

Because CorEx-Servpro is a critical vendor, they must have a solid BC/DR plan that is tested and reviewed at least annually. The last review of the BC/DR plan took place four months ago. The plan was deemed sufficient by an SME.

As a critical vendor, they must undergo risk and performance monitoring and review on a quarterly basis.

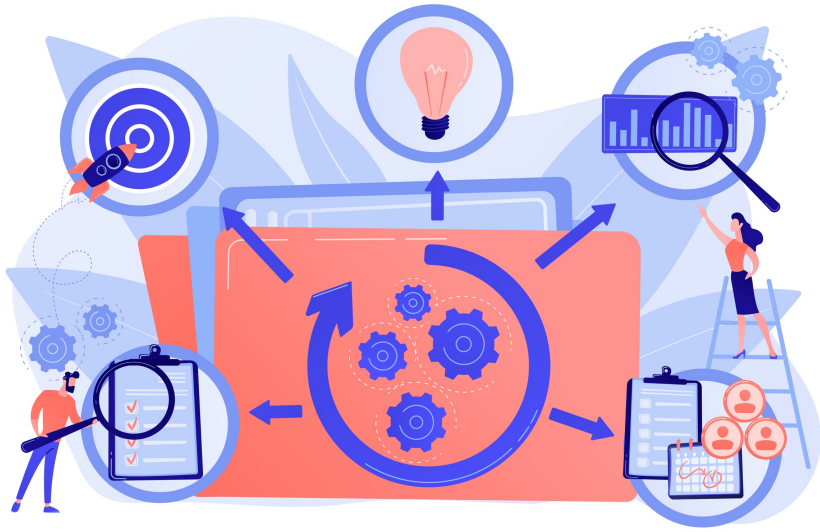
venminder

CorEX-Servpro – A Case Study

Continued

- **Missed SLAs:** When a vendor fails to meet agreed-upon Service Level Agreements (SLAs), it could indicate that their current systems, processes, or tools are not effective or are deteriorating. If they are unable to provide required services or products in a regular business environment, it is doubtful they will be able to deliver them during or after an event.

- **Unverified Controls:** If the information validating the existence and effectiveness of vendor controls is expired, there is no way to know if the controls are still sufficiently addressing the known risks. Failed or ineffective controls can cause unwanted events such as system outages, data breaches, data loss, regulatory violations, loss of customers, and more.



venminder

CorEX-Servpro – A Case Study

Continued

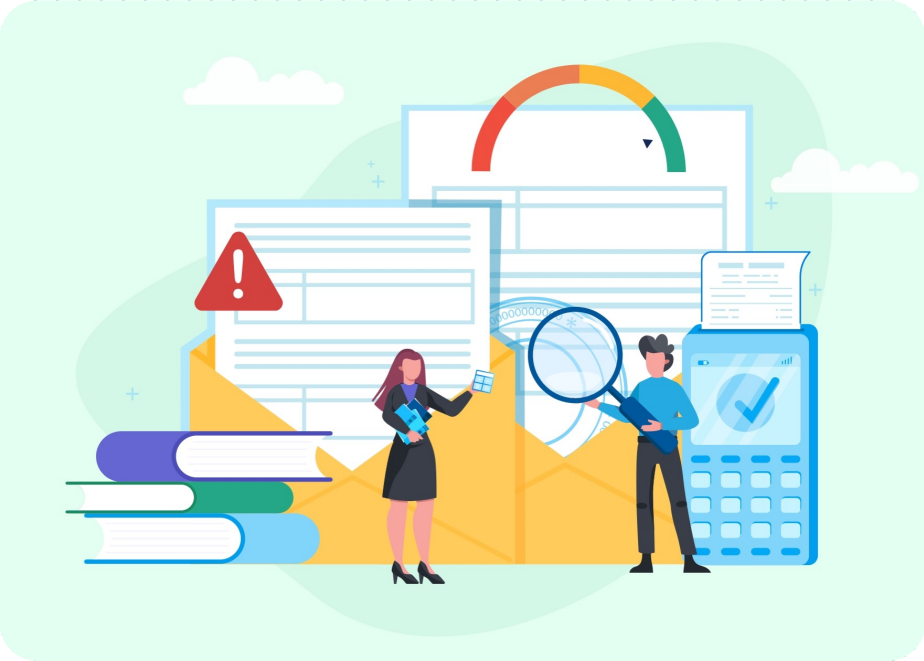
- **Declining financials:** Financial issues may indicate that trouble is brewing. In tough financial times, a vendor may need to reduce staff, limit focus on products or services delivered to your organization, or become unable to meet contractual requirements, which can reduce the effectiveness of a BC plan.

- **Loss of Key Staff:** Loss of essential skills and knowledge may occur due to key staff changes, and inexperienced employees can negatively impact the successful execution of a BC/DR plan. The plan may also list outdated contact information- which is useless during an emergency.

- **Poor Cyber Hygiene:** A lack of constant and consistent data security can result in business interruptions or data loss due to cyber breaches or hacking incidents.

venminder

Business Continuity and Disaster Recovery and the Link to Risk and Performance Monitoring



Monitoring your vendor's risk and performance is essential to identify issues that could ultimately make or break the vendor's ability to resume operations, preserve data, protect your customers, and meet regulatory requirements during and after a business interrupting event.

venminder

Common Issues That Can Impact Your Ability to Monitor Vendor BC/DR Properly

Some factors may hinder alignment between your risk and performance monitoring and the vendor's BCP, including:

- The vendor owner never reads the plan – unless there is an emergency (which might be too late)
- An SME reviews vendor BCPs, and they are filed away until the next review
- BCPs are not tested or results of BC planning are not shared with your organization
- Discussions of BC planning and testing are not included as part of regular vendor performance reviews
- Current employee work schedules and locations are not reflected in the plan
- Vendor personnel changes are not made known to your organization, making it difficult to validate current BCP contact lists and call trees
- Fourth and nth parties relevant to the vendor’s BCP are not disclosed or included in the plan
- The vendor has poor TPRM practices (no risk assessments, due diligence, or monitoring)
- Open vendor risk or performance issues are not tracked or managed

Risk Monitoring

Risk monitoring is a multi-layered activity that considers the following elements.

- Known risks (as identified in the inherent risk assessment)
- New or emerging risks (including industry issues or changes in regulatory expectations)
- Sufficiency of the vendor's control environment (risk management practices and controls)
- Vendor performance
- Regulatory compliance
- Disclosure of relevant fourth and nth parties
- Contractual requirements
- Fourth and nth Parties
- Open issues and remediation

Risk Monitoring Processes and Tools

Periodic Risk Monitoring should take place on a regular and predictable schedule.

- Critical and High-Risk – at least annually
- Moderate – 18 months to two years
- Low – recommended at least every three years or before contract renewal

Risk Re-Assessment – Validation of the inherent risk questionnaire. Has anything changed?

Confirmation of Vendor Risk Questionnaire – Has anything changed? Are the same controls in place?

Due Diligence Review/ Control Assessment

- Are the documents you have the most current?
- Are independent audits, insurance, and licensing up to date?
- Are the vendor's controls still in place and effective?
- Has the BCP been tested, and if so, what were the results?
- What is the financial status of the vendor
- Is the vendor's list of relevant fourth and nth parties current?
- Can the vendor prove they are risk assessing, performing due diligence, and monitoring their vendors?

venminder

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

venminder

Risk Monitoring Processes and Tools

CONTINUED

Other risk considerations:

- Has there been any change to management or key personnel?
- Where are employees performing their work? (Working from home, office, hybrid?)
- Have there been any issues or incidents?
- What is the status of the contract?
- How has the vendor been performing? (Poor performance is often a sign of new or emerging risks)

venminder

Risk Monitoring Processes and Tools

CONTINUED

Continuous risk monitoring is an ongoing activity that requires constant awareness of the vendor's status and reputation. During continuous monitoring, you are looking for:

- Negative news about the vendor
- Negative news about the vendor's subcontractors (your fourth and nth parties)
- Changes to the vendor's industry
- Cyber events and breaches
- Regulatory changes
- Customer complaints
- Enforcement actions
- Change in ownership
- Changes to management or key personnel
- Changes in performance
- Changes in consumer behavior
- Lawsuits
- **And more…**

venminder

Risk Monitoring and BCP Considerations

Risk monitoring enables better BC/DR planning because you can identify problems that might prevent successful BCP execution during or directly after a business interrupting event. It is recommended that you carefully read and understand vendor BC/DR plans and pay special attention to the following:

- **Cyber and data security, availability, and confidentiality:** Data loss and theft can occur because of cyberattacks, system breaches, failed controls, improper access management, or poor data security hygiene. Identify how data backup and restoration are to be handled per the BC/DR plan and validate that the vendor's current controls are sufficient.
- **Changes to management or key personnel:** Organizations typically empower specific individuals to activate and execute the BC/DR plan. If those individuals leave the organization, make sure the plan is updated and that the vendor confirms new employees have been appropriately trained and can execute the BC/DR plan appropriately.
- **Fourth and nth parties:** Vendors must disclose relevant subcontractors who are instrumental in providing products and services to your organization. The vendor's BCP should account for those fourth and nth parties and the role they play (if any) in the vendor's BC/DR planning. It is essential to validate that the vendor is properly managing these relationships.
- **Vendor financial health:** Decreasing financial health may jeopardize BC/DR plans if there is a shortage of staff, reduced investment in cybersecurity, or closure of backup sites or systems.

Using Vendor Risk Alert and Monitoring Services

An effective way to gather continuous monitoring information is through professional vendor risk alerts and monitoring services. Using these services should provide more relevant and timely information than depending on just internet news alerts alone. These services can be utilized at different times and in different ways, including:

To provide a quick report on a current vendor's financial status, cybersecurity posture, regulatory compliance, litigation status, geopolitical issues, or other risk dimensions. These reports can be used as pre-due diligence in RFPs and RFIs or to validate your existing due diligence or risk monitoring efforts.

To provide targeted risk alerts for specific vendors or their subcontractors.

- Changes to a vendor's cybersecurity posture
- Data breaches or cyber incidents
- Regulatory enforcement actions
- Significant litigation
- Changes in a vendor's financial health
- Negative news and issues concerning a vendor's reputation
- Mergers and acquisitions
- Changes to the vendor's industry (new regulations, laws, etc.)

venminder

What Vendor Performance Management Is

1. The routine process of ensuring your vendors deliver their products and services as expected

2. Verifying products and services are delivered on time with the right level of quality and at the agreed-upon price

3. Ensuring that the vendor relationship is helping your organization achieve its strategic goals

venminder

Why Vendor Performance Management Is Important

1. Enables early detection of emerging risks before an incident occurs
2. Confirms the vendor is fulfilling the terms of the contract and delivering value in the relationship
3. Enhances vendor comparison data

Who Should Be Responsible for Evaluating Vendor Performance

- **Vendor Owners** have the responsibility for the evaluation and management of vendor performance, managing issue remediation, and holding the vendor accountable. They should also establish and formalize all Service Level Agreements (SLAs), Key Performance Indicators (KPIs), and Key Risk Indicators (KRIs) in collaboration with the vendor.

- **Third-Party/Vendor Risk Management** oversees vendor performance management reporting on the results, documenting, and tracking vendor issues, and holding the vendor owner accountable.

- **Senior Management** is responsible for enforcing the policy and holding the vendor owners, the business lines, and third-party/vendor risk management accountable for executing the process per the policy and should be informed of performance issues for vendors deemed as critical.

venminder

4 Key Components of Performance Management

1. **Established and agreed-upon SLAs and KPIs**
   - Contract
   - Industry standards and norms
   - Verbal or written agreements outside of the contract

2. **Performance data collection and reporting (Scorecards)**
   - Agreement on measurement data type, source, and format
   - Both parties can review data

3. **Performance review meetings**
   - Established meeting routines and timing
   - Documented meeting notes, actions, issues, and timing

4. **Issue management with time-bound tracking and closure**
   - Performance issues are tracked and managed
   - All remediation is time-bound, routine escalations of “at risk” or “past due” issues

venminder

Service Level Agreements (SLAs)

- SLAs are an agreement to provide a specified level of service.
- SLAs establish firm, legally binding commitments between your organization and the vendor.
- SLAs represent "non-negotiable" service requirements that are identified and outlined in your contract or other written agreement.
- With SLAs, there is often a requirement for remedy or a stated penalty in case the vendor doesn't meet the commitment, such as a refund, service credit, or discount.

venminder

SLA Examples

SERVICE LEVEL AGREEMENTS CAN ADDRESS ANY MUST-HAVE FACTOR OR REQUIREMENT IN THE ENGAGEMENT.

Examples include:

- Response Time
- Repair Time
- Accuracy
- Quality
- Safety
- Cost
- Cybersecurity Controls
- Customer Satisfaction
- System Uptime
- Breach Notification

NOT ALL SLAS ARE DESIGNED TO BE PUNITIVE.

Certain industries (customer service, sales, and collections, for example) may have service level agreements to incent stronger performance.

***Example*:** For every month the customer call center averages > 90% customer satisfaction, a 10% bonus will be paid to the vendor.

venminder

Key Performance Indicators (KPIs)

- KPIs are meant to measure the performance aspects that help your organization meet its goals and objective.
- KPIs are metrics that assess how well a vendor performs business functions, progresses towards a goal, or achieves objectives.
- KPIs measure something that has already happened – **they are a lagging indicator.**

You don't need a KPI for every vendor action or output, but only for those outputs, actions, deliverables, or behaviors that help your organization meet its objectives and validate the service levels of the vendor.

venminder

Key Risk Indicators (KRIs)

- Key risk indicators are metrics that predict potential risks that can negatively impact your business
- **KRIs are a leading indicator** – meaning they can tell you about something that hasn't happened yet
- KRIs can serve as a control by identifying potential issues before they become big problems
- Can be validated through reliable, available, accurate, and timely data
- Be S.M.A.R.T (specific, measurable, achievable, realistic, and time-bound)
- Establish trends or show patterns over time
- Be created in partnership with the vendor

venminder

Vendor Performance Metrics

- Identify possible vendor performance metrics
- For each KPI, identify an associated KRI
- Articulate the rationale for each metric

This approach increases the value of the metric reporting overall.

Metric	KPI Rationale	KRI Rationale
% of Uptime	• Meeting SLAs • Data availability • Customer satisfaction	Patterns of decreased or declining uptime can result in: • Business interrupting events • Audit or exam findings/actions/fines • Customer dissatisfaction • Financial loss

venminder

Integrating BC/DR Into Vendor Risk and Performance Monitoring

When reviewing your vendor's BC/DR plan, consider the elements required to execute and monitor the plan successfully. This could include:

- Evidence of regular data backups
- Validated vendor contact list and information
- Personnel loss and planning strategies
- Relocations plan
- Remote access availability
- Critical fourth and nth parties
- Changes to policies such as hybrid or remote work
- Current pandemic prevention measures
- Open issues and remediation progress

venminder

Formal Vendor Performance Reviews

While you must monitor the vendor's performance constantly and address issues as they arise, you also need to formally review the vendor's performance with the vendor on a regular schedule.

HERE ARE THE RECOMMENDED MINIMUM REVIEW INTERVALS:

- **Critical or High Risk:** At least quarterly
- **Moderate Risk:** 1-2 times a year based on the product or service
- **Low Risk:** Due to the nature of the products and services rated as low risk, you may not need to manage or review performance. This is at the discretion of your organization. It's recommended that you consider the vendor's performance before renewing contracts or placing new orders.

venminder

Performance Review Meetings

PREPARE:

- Collect and populate scorecard SLA, KPI, and KRI data
- Provide a copy of the completed scorecard to the vendor
- Schedule a review meeting

REVIEW MEETING:

- Review all data – take notes!
- Review issues, root causes, and vendor remediation plans
- Determine next steps
- Finalize the meeting by adding vendor owner comments – provide a final copy to the vendor
- Store scorecard and meeting notes with the vendor record

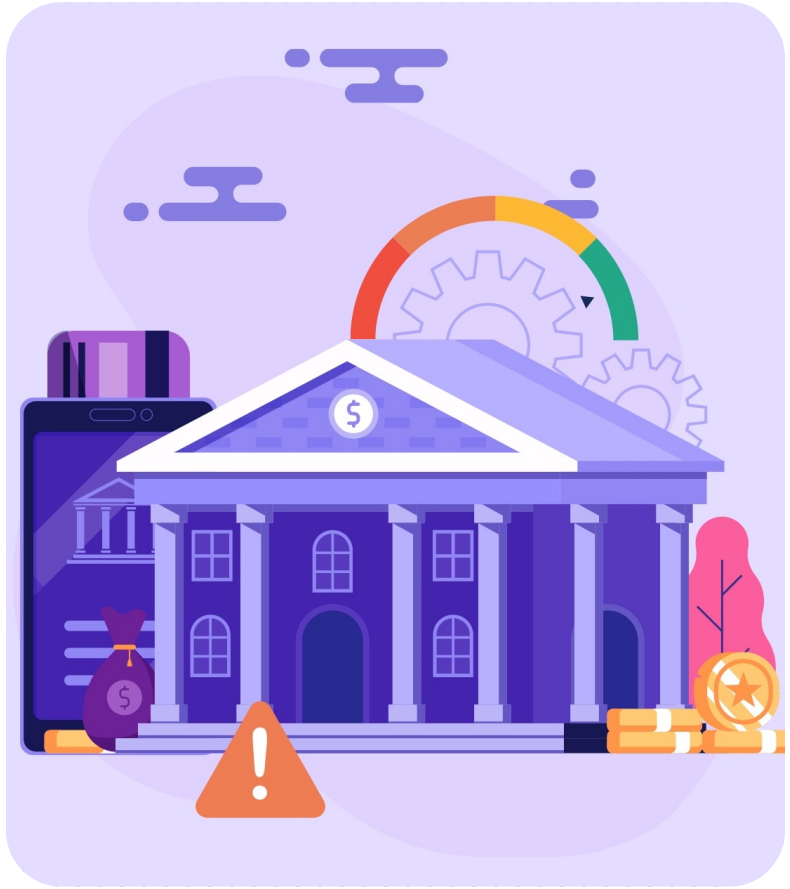
RETAIN DOCUMENTED EVIDENCE OF PERFORMANCE MANAGEMENT:

- Meeting invites/attendees
- Meeting notes
- Completed scorecards
- Review meeting notes
- Remediation plans
- Vendor presentations

Create a Remediation Strategy

If a vendor fails to meet performance standards, a remediation plan must be developed immediately. In most cases, the vendor should be able to provide the following details:

- Summary of the issue, including duration and impacts
- The root cause or why the issue occurred
- Plan of action for remediation
- Remediation timing



PRO TIP: It's essential to formally document any failed performance as an open issue and track the remediation until it's resolved. If your organization fails to take corrective action, you're further exposed to ongoing or expanded vendor performance risk.

venminder

Why Issue Management Is Important

Failing to address vendor issues will only cause you and your organization more problems.

The following are 6 reasons why managing vendor issues is important:

1. **Protects your reputation:** If a vendor is experiencing many issues, and/or receiving complaints due to the issues, your customers will start to notice, and your organization will take the blame, resulting in your own reputation being impacted – especially if they're a customer-facing vendor.

2. **Minimizes risk to operations and customers:** If issues arise with vendors who are critical to operations or the services you provide to your customers, there is a risk to operational integrity and resilience.

3. **Meets regulatory expectations:** Regulators require you to have a mechanism in place that creates a standardized process to identify, manage, and remediate issues. Adequately responding to vendor issues is a best practice and both a customer and regulatory expectation.

Why Issue Management Is Important

4. **Ensures contractual obligations are being met:** To ensure your vendors are meeting their obligations – including service level agreements (SLAs) and other expectations – you must track and review any issues that occur to have a good handle on when and why they're in breach. If SLAs aren't being met, a log of the issues helps when evaluating the vendor's plans to address the underlying issues. It may also trigger your own continuity and/or exit plans.

5. **Assists with contract renewals:** Having the ability to see vendor issues, in detail and at any given time, helps when determining if the vendor is still the right fit or not, and may even provide you with some leverage during contract negotiations.

6. **Ensures the vendor has proper controls in place to protect data:** Noticeable vendor issues can be the result of underlying operational problems, which could then affect the quality of information security. When a vendor lacks proper controls, they often experience data protection issues. A process for managing issues will help you highlight vendors struggling in this area. This is especially important if it's a recurring problem.

Examples of Discovering Vendor Issues

- **Due Diligence –** You're reviewing a vendor's BC/DR plans and you discover that findings within their last DR test haven't been addressed. This is a major concern, especially if the vendor is critical to your ongoing operations. It should be tracked as an issue and followed up on.
- **Monitoring –** Performance has been degrading over several cycles and your vendor owner doesn't feel contractual obligations are being met.
- **Monitoring for Risk –** There's been deterioration in your vendor's financial condition.
- **Actual Events –** Your vendor has had or caused security breaches, data loss, service, or system interruptions.
- **Termination –** You haven't received the formal certificate of destruction (COD) from a vendor that was hosting your data.

venminder

Recommendations to Help With Remediation

- **Keep a conversation and document log.** Log all communication regarding the issue at hand as well as keep all documents and emails centralized in one location.

- **Determine an action plan.** Work with the vendor to ensure issues are resolved. This could include implementing new controls, increased monitoring and due diligence, contract amendments, more regular follow up meetings, etc.

venminder

Recommendations to Help With Remediation

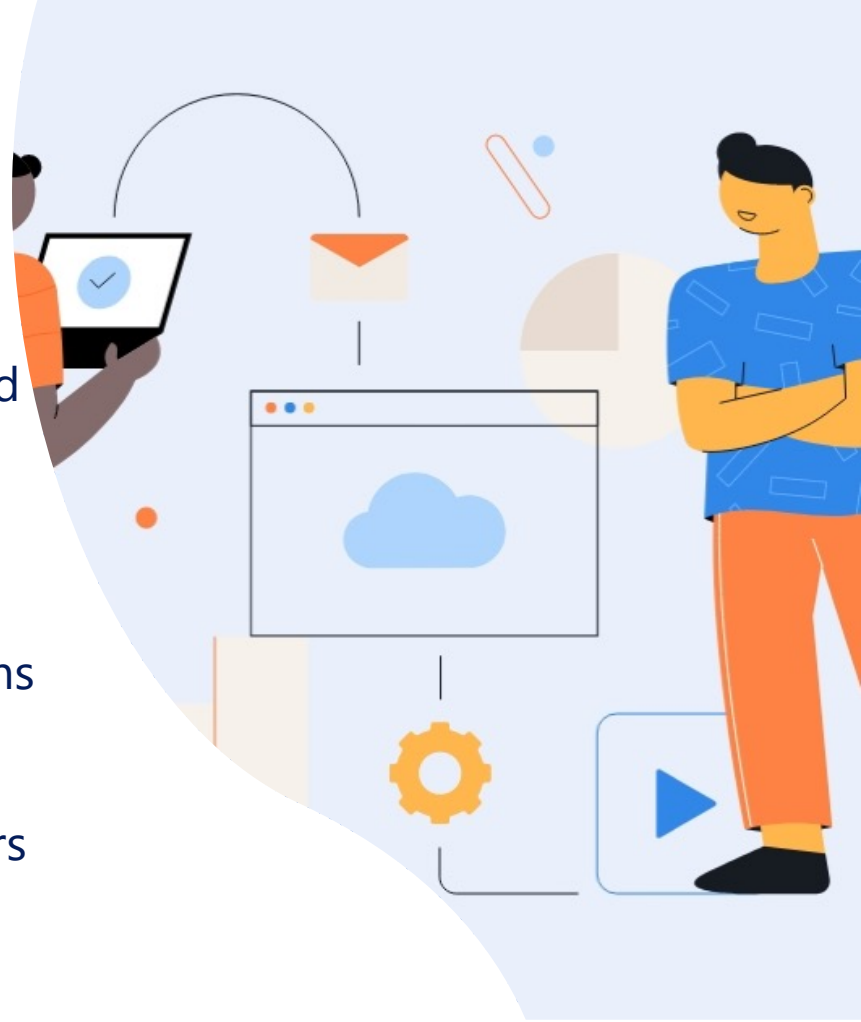
- **Escalate and/or terminate as needed.** If you can't resolve the issue, or come to a mutual agreement, you may need to take further action, which can include escalating to the board, seeking a new vendor/termination, referring to the exit strategy, etc.

- **Report on the issue.** Run reports on vendors that shows all in progress and resolved vendor issues, and share that with senior management and the board, as needed. This is an easy way to flag problem vendors, spot trends, and keep them informed.

Strong Vendor Issue Management

Strong vendor issue management ensures:

- Increased visibility into your overall risk profile (e.g., issues related to performance)
- Triggers for exit plan testing and/or implementation
- An opportunity to negotiate better pricing or other contract terms and conditions due to poor performance or other issues
- Improved reporting to the board, committees, examiners/auditors
- The ability to terminate a vendor relationship due to breach of contract and underlying service level agreements
- Lessons learned and the long-term insight into recurring vendor problems and/or opportunities to improve your third-party risk management processes



Key Takeaways

- Risk and performance monitoring are integral to successful BC/DR planning and execution
- Vendor issues that exist in a business-as-usual environment will become amplified in a business-interrupting event
- Vendor owners and third-party risk management teams must read and understand BC/DR plans for critical and high-risk vendors
- Validate BC/DR plan components as part of your ongoing risk and performance monitoring
- Issue management is essential – failure to address known issues effectively can negatively impact BC/DR plan execution

venminder

THANK YOU

Questions & Answers

POST A QUESTION:
www.thirdpartythinktank.com

THIRD PARTY thinktank
A Community for Risk Professionals

EMAIL US:
resources@venminder.com

FOLLOW US:
@venminder

venminder