Bridging the Gap: 4 Tips for Integrating TPRM and Business Continuity

You may feel confident that your bank is prepared for an unexpected incident, but what about your vendors? If your institution relies on a third-party service provider (TPSP) that struggles to recover quickly from a disaster, there is a significant gap in your business continuity management (BCM).

Banks must acknowledge the connection between vendor management and business continuity. The Interagency Guidance on Third-Party Relationships: Risk Management emphasizes the importance of a vendor's operational risk management and resources in key areas such as BCM, disaster recovery plans, and resiliency testing. However, integrating vendor management with business continuity isn't just a compliance checklist; it enhances your bank's overall safety, strength, and preparedness.

How can your bank integrate these two vital areas? Here are four best practices to implement as you revisit your TPRM program and BCM strategies.

1. **Coordinate Policies Across the Institution**

Develop your business continuity plan (BCP) alongside your vendor management policies. Too often, departments work in siloes, resulting in miscommunication, duplicated efforts, and general confusion. To prevent these problems, use the same language and definitions and align with your bank's larger risk management strategic objectives and goals.

When compliance and TPRM work together at the policy level, your bank creates better results.

2. **Use Proper Risk Assessment Methods**

Vendor risk assessments are essential during the due diligence phase of managing vendor relationships. Before conducting a vendor risk assessment, first identify critical vendors. While it's tempting to assign a "critical" or "high-risk" rating to many vendors, limit the designation of critical vendors to those presenting a significant risk. For guidance on designating critical third-party activities, refer to the Interagency Guidance.

Once you've identified critical vendors, you'll know how deep due diligence must go. (Critical vendors require deeper due diligence.) Analyzing documentation like service organization control (SOC) reports and financial statements to identify potential business continuity risks leads to better decision-making and protective controls. Vendor risk assessments should be updated when changes in operations, regulations, or risk profiles occur.

3. **Analyze Agreements**

The best time to mitigate risk is when a contract is first formed. Business continuity and vendor management should work together to define requirements and expectations before negotiations. This shared process should include clarity on audits, documentation, and timelines for deliverables, including recovery time objectives (RTOs) and recovery point objectives (RPOs).

Move beyond just taking a vendor's word on compliance — ensure you have the necessary due diligence and verification tools. Remember, your vendors' risk is your bank's risk, too.

4. **Monitor Proactively**

Regulators expect your bank to monitor your vendors continuously. Ongoing monitoring ensures the strength of your vendors' risk and compliance controls over time and that third parties follow through on their contractual obligations and service standards.

The business continuity planning and vendor management teams should share monitoring responsibilities and findings. Include annual reviews (e.g., required vendor documents like SSAE 18s, disaster recovery plans, and financial evaluations) and continuous monitoring for issues that could add to vendor instability such as litigation, data breaches, regulatory concerns, and overall financial performance.

Integrating TPRM and business continuity is a recipe for a strong, adaptable organization that can withstand the inevitable disruptions that every financial institution faces. By implementing these best practices, you can strengthen your bank's resilience and ensure that your vendor partnerships contribute positively to your business continuity strategy.