Financial Regulators Release New Appendix to Business Continuity Planning Booklet

The FFIEC released a revised Business Continuity Planning (BCP) Booklet, which is part of the FFIEC Information Technology Handbook (IT Handbook). The update included an addition of appendix J, Strengthening the Resilience of Outsourced Technology Services.

What does this mean for Financial Institutions?

Financial Institutions must ensure that they properly vet third parties who provide operational and technology services in regards to their Business Continuity Planning (BCP). The new appendix discusses four key elements of BCP that a Financial Institution should address:

1. **Third Party Management**
   Third party management programs should be risk-focused and provide oversight and controls to commensurate with the level of risk presented by the outsourcing arrangement.
   a. Proper due diligence
      i. Consider the maturity of new technologies
      ii. Gain an understanding of the benefits and risks of engaging the third party
      iii. Assess the effectiveness of the third party's business continuity program
         1. Focus on recovery capabilities and capacity
      iv. Understand the due diligence process that the third party uses for its subcontractors and service providers
      v. Review the third party's BCP program
         1. Ensure it aligns with the Financial Institution's own program
         2. Evaluate the third party's BCP testing strategy and results
   b. Proper contract management
      i. The terms of the contract should be defined in written contracts that have been reviewed by the Financial Institution's legal counsel and subject matter experts before execution.
      ii. There are several contract terms specifically mentioned in the FFIEC Appendix: right to audit, establishing and monitoring performance standards, default and termination, subcontracting, foreign-based service providers, BCP testing, Data governance, service provider updates and security issues.
   c. Ongoing monitoring of Technology Service Providers
      i. Ensure that management effectively monitors third party performance throughout the life of the contract. This includes periodic, in-depth assessments of the third party's control environment, BCP and Information Systems.
      ii. Financial Institutions should ensure business reliance considerations are imbedded in the ongoing monitoring and it is well documented.

2. **Third Party Capacity**
   The increased use of third party service providers by Financial Institutions and the consolidation of the industry has resulted in fewer service providers providing services to larger number of Financial Institutions. If several Financial Institutions are involved in a natural disaster, does the third party have the capacity to support recovery services to large numbers of Financial Institutions?

3. **Testing with Third Party Technology Service Providers**
   When a third party provides important services to a Financial Institution, it should be included within the Financial Institution's enterprise-wide business continuity testing program. The testing program should be based on a Financial Institution's risk prioritization and criticality of the functions involved, which is determined through risk management activities.

4. **Cyber Resilience**
   Financial institutions and their third parties must incorporate the potential impact of a cyber-event on their BCP process and ensure appropriate resilience capabilities are in place. Incident Response must also be developed. The appendix describes a number of risks that must be managed: malware, insider threats, data or system destruction and corruption, communication infrastructure disruption and simultaneous attack on Financial Institutions and third parties.

For more detail and information pertaining to this, other FFIEC releases or Cybersecurity in general, please contact one of the following individuals in your market:

Shane O'Donnell, Michigan – sodonnell@makopro.com
Brooke Gardener, NE Indiana, NW Ohio – bgardener@makopro.com
Peter Clarke, Indianapolis, Cincinnati, Chicago – pclarke@makopro.com