ICBA
INDEPENDENT COMMUNITY BANKERS of AMERICA®

December 11, 2019

Key Updates to the FFIEC BCM Booklet

The Federal Financial Institutions Examination Council (FFIEC) released an updated version of its *Business Continuity Management Booklet* one of a series of booklets which make up the *FFIEC Information Technology Examination Handbook (IT Handbook)*. While the IT Handbook is "prepared for use by examiners," it is also an essential resource for community banks who can use the information to better prepare for regulatory examinations.

Upon reviewing the new booklet, the changes may be overwhelming. The FFIEC has done a tremendous amount of work reorganizing and restructuring the document. However, closer examination will find much of the same content from the old Booklet in a simpler, more logical format which allowed the FFIEC to take a deeper dive into some key areas of business continuity management. This resource will outline the key updates to the BCM Booklet that community banks should be aware of.

Management

First and foremost, the title has changed from *Business Continuity **Planning*** to *Business Continuity **Management***. The FFIEC's goal is to "reflect the expanded role of information technology (IT) plays in supporting business operations and meeting customer expectations." A growing trend is to prepare organizations to be operationally resilient during a crisis. This means not only being able to plan for your business continuity, but to further understand how you can manage your business through a crisis with minimal impact on your business operations and your customers' experiences.

Restructuring

The past few updates to the booklet have mostly been adding appendices to cover emerging trends of business continuity management. In this update, the FFIEC has restructured the booklet to incorporate the added appendices into the main document to create a clearer and more concise set of expectations. Of note, the former Appendix J, which outlined third party risk management is now integrated into the main document.

Board Reporting

The old Booklet spread expectations for the Board of Directors throughout the document. In what should come as a welcome change, the new version consolidates the expectations for Board of Directors' oversight into a section of its own. Key points to note in this section are that while it does not require annual, formal reports to the Board, it does require a "written presentation providing the BIA, risk assessment, BCP, exercise and test results, and identified issues." Also, that "Board minutes should reflect business continuity discussion (including credible challenges) and approvals."

Exercising

Exercising of all sorts, discussion-based, range-based, even surprised drills, have become a more common practice in recent years. The new version of the Booklet sets clearer explanations of what is expected from testing and exercises, bringing in the expectations found in the appendices into the main document. Additionally, the Booklet provides industry resources which they suggest partaking in. These include FS-ISAC's Cyber-attack Against Payment Systems (CAPS) exercises as well as the US Department of the Treasury's Hamilton Series.

Resilience

A new section of the booklet focuses on resilience by bringing together information originally located in the former appendices; largely Appendices E (interdependencies) and J (third parties). The section outlines physical and cyber resilience, as well as data backup and replication, personnel, third-party service providers, telecommunications, power, change management and communications.

An important section to take note of is “Data Back up and Replication.” The booklet suggests "Entities should develop appropriate cyber resilience processes that enable restoration of critical services if the institutions or its critical service providers fall victim to destructive cyber-attack or similar event…An example of an industry initiative to assist in addressing the resilience of customer account information is **Sheltered Harbor**." Sheltered Harbor is voluntary industry initiative which promotes financial sector resilience through a combination of secure data vaulting of critical customer account information with a comprehensive resilience plan to provide customers timely access to their account information and underlying funds during a prolonged systems outage or destructive cyber-attack.

Business Continuity Planning

Compared to the 2015 version, the FFIEC dove much deeper into the principles and requirements of putting together a proper Business Continuity Plan (BCP). While high level concepts of BCPs were previously included, this version provides more details on the components as well as the business operations that banks should consider in their BCP (payment systems, liquidity considerations, branch relocations, data center recovery). Additionally, the update They’ve borrowed a lot of concepts and definitions from NIST, including the establishment of an incident response team, which was not included in previous versions. Additionally, the update outlines expected response mechanisms such as incident response teams, disaster recovery and crisis/emergency management.