Cybersecurity Assessment Tool Comments

We would like to thank the FFIEC for allowing financial intuitions to comment on the new Cybersecurity Assessment Tool. We had the opportunity to complete the FFIEC's Cybersecurity Assessment Tool and offer the following comments. These comments are not all inclusive; they are a sampling of concerns we see with the documents.

General Comments

It seems the Cybersecurity Maturity Domains are purposely written so that a community bank can not reasonably, in a cost effective manner, achieve the Innovative maturity level. We are confused why the bar would be set so high as to be unattainable.

It would be very helpful if the Cybersecurity Maturity worksheet was a Word document.

- It can be completed once and updated as changes occur in the bank i.e. launching new products or services, new connections, etc.

- Since it is generally completed by someone other than senior management, it is helpful to be able to insert comments under the various questions so management knows why a question was answered the way it was. This is particularly important since the document states it is supposed to be a measurable and repeatable process. Easier to be repeatable if the document can be updated electronically rather than redone each time.

It would be beneficial to have an annotated Cybersecurity Maturity workprogram. While cross referencing to the FFIEC's Information Technology handbook and NIST is nice, it is not enough information. Providing more of what the FFIEC is specifically looking for would be better. Comments like "as cybersecurity relates to other critical infrastructures" appears many times throughout the Advanced and Innovative sections - what specific examples are the FFIEC looking for? Community banks can not even get basic information (i.e. back up/resiliency plans, external audits, etc.) from large vendors that are not IT specific vendors. How are community banks supposed to get information from large, non-IT specific, yet still mission critical service providers?

How is a community bank supposed to "promote cybersecurity culture across the sector and other sectors that they depend on" – Page 29, Innovative section of Cybersecurity Maturity: Domain 1. The workprograms should provide specific, real world examples that can be reasonably expected to be achieved by a community bank.

It appears this is trying to be a one size fits all document and it is unsuccessful in that endeavor. Community banks are not the same as the multi-national/multi-regional financial institutions. The documents, specifically the Cybersecurity Assessment Tool – Cybersecurity Maturity workprogram, should be either tiered for community banks and large banks or a separate workprogram for community banks. Structuring it in tiers like the IT Handbook workprograms would be beneficial.

Users Guide

Page 1 of the Users Guide states in the first paragraph that the Assessment "…to help institutions identify their risks and determine the cybersecurity maturity." However, the last sentence in the third paragraph states "…the Assessment is not designed to identify an overall cybersecurity level." It seems inconsistent. Either the tool will identify the maturity level or it won't. If it won't, then what is the purpose?

Cybersecurity Assessment Tool Comments

Cybersecurity Maturity Workprogram

The way the Maturity workprogram is written, if a bank can't answer yes to every question, then that section can not be noted as that level being complete. For community banks, that is grossly unfair. Specific examples include:

Page 22, Advanced section, community banks do not have separate cybersecurity standards; those are incorporated into information security. That section also states the "risk appetite is informed by the instruction's role in critical infrastructure." What specifically is the FFIEC looking for? What type of measurable and repeatable process would be appropriate here for a community bank?

Page 24, Advanced section, community banks do not have independent risk management staff. Risk management is part of every employee's duties. There are specific people that have overall responsibility for risk management, but they also have many other duties and responsibilities.

Page 24, Innovative section, how would a community bank analyze the financial impact a cyber incident has across the financial sector? Is this a realistic expectation for a community bank?