INDEPENDENT COMMUNITY BANKERS of AMERICA®

Preston L. Kennedy, *Chairman*
Noah W. Wilcox, *Chairman-Elect*
Robert M. Fisher, *Vice Chairman*
Kathryn G. Underwood, *Treasurer*
Alice P. Frazier, *Secretary*
Timothy K. Zimmerman, *Immediate Past Chairman*
Rebeca Romero Rainey, *President and CEO*

June 4, 2019

Chief Counsel's Office
Office of the Comptroller of the Currency
Attn: 1557-0328
400 7th Street SW, Suite 3E-218
Washington, D.C. 20219

Submitted via email: prainfo@occ.treas.gov

Re: Office of the Comptroller of the Currency, Agency Information Collection Activities: Information Collection Renewal; Comment Request; FFIEC Cybersecurity Assessment Tool, OMB Number 1557-0328

Dear Sir or Madam:

On behalf of the Independent Community Bankers of America,[1] we appreciate the opportunity to provide information on behalf of community banks to the federal banking regulators about the Federal Financial Institutions Examination Council's ("FFIEC") Cybersecurity Assessment Tool ("CAT"). To obtain information requested in the Paperwork Reduction Act Notice, ICBA solicited feedback from members of its Subcommittee on Cyber and Data Security ("ICBA Subcommittee" or "Subcommittee"), which includes institutions between $100M to $2B in assets.

Community banks, like the entire financial services sector, takes seriously their responsibility to protect customer information and their own systems against cyber threats and vulnerabilities. ICBA is appreciative of the FFIEC's willingness to continually evaluate and review the effectiveness of the CAT, including revisions that have been made to improve its utility.

[1] *The Independent Community Bankers of America® creates and promotes an environment where community banks flourish. With more than 52,000 locations nationwide, community banks constitute 99 percent of all banks, employ more than 760,000 Americans and are the only physical banking presence in one in five U.S. counties. Holding more than $4.9 trillion in assets, $3.9 trillion in deposits, and $3.4 trillion in loans to consumers, small businesses and the agricultural community, community banks channel local deposits into the Main Streets and neighborhoods they serve, spurring job creation, fostering innovation and fueling their customers' dreams in communities throughout America. For more information, visit ICBA's website at www.icba.org.*

Recommendations

ICBA suggests the agencies implement the following recommendations, which are detailed below:

1. Continue to stress that the use of the CAT by financial institutions is voluntary and that banks may continue to follow the guidance in the FFIEC IT Handbook, which states that institutions can reference one or more recognized technology frameworks.[2]
2. Provide banks an automated or interactive document to input information for the CAT, as opposed to a static PDF document of questions and responses.
3. Provide community banks benchmarking information during IT Examinations.
4. Revise the linear nature of the inherent risk review.

Voluntary Nature of the CAT

Of the community banks that responded to our request for information, several banks indicated that examiners merely provided a cursory review of the CAT, if at all. When examiners reviewed the CAT with the bank staff, bankers responded that examiners spent between thirty minutes to one hour reviewing the document. The prudential regulators should clarify that if institutions take the time to complete the CAT, then examiners should spend time reviewing the CAT with the institution. If examiners complete the CAT as part of the examination process, then the CAT completed by the examiner should be reviewed with the institution during the exam.

Provide a Usable Format

Many community banks are using the Financial Services Sector Coordinating Council's automated CAT spreadsheet to complete the CAT in advance of their examinations. Community banks have requested that the FFIEC provide the CAT in a usable format, one that can be easily completed and provided to the examiner, if requested.

Benchmarking

An advantage to the broad collection of this information across the entire financial services sector is the ability to compile information into useful benchmarking data for banks of comparable size and risk profiles so that peer institutions may become aware of their overall cybersecurity posture in the sector. This information may be useful to an information security officer or board of directors, particularly when it comes time to discuss budget impacts of the bank's security posture. Additionally, benchmarking may allow the regulators insight into broad categories of risk and exposure in the financial services sector. Working with public-private partnerships, this information could also be shared to help develop defenses against any sector vulnerabilities.

---

[2] Federal Financial Institutions Examination Council, IT Handbook, Information Security Booklet. II.C.4: "Control Implementation". September 2016. See https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic4-control-implementation.aspx

Linear Nature of Inherent Risk

One banker commented that the inherent risk review is very linear and could be better rooted in bank operations and market conditions. The banker advocated for an "if-then" consideration with the inherent risk determination. As an example, consider that many community banks currently engage cloud providers for data management. While cloud computing is a standard term, not all cloud computing companies are equal (i.e. they do not all have the same risks based on their own mitigating controls). While a bank may check the "most" risk level due to the sheer number of cloud providers, the CAT should allow for an additional level of risk mitigation, such as vendor management and vendor type, which could significantly reduce the risk.

Usage of the CAT

Community banks employ the CAT as one of the tools they use to assess their cybersecurity risk and maturity. However, not all banks use the CAT exclusively. Most banks use the CAT in conjunction with other recognized technology frameworks. As such, examiners should not require the use of the CAT nor require the institution to translate any risk framework they use into a CAT format. If the regulator is requiring the examiner to complete the CAT, then the examiner should translate the framework into the CAT format.

Burden – Time and Cost

As mentioned previously, the ICBA Subcommittee represents institutions between $100M-$2B in assets. The time to complete the CAT was reported as being 40 hours or less depending more on the risk and complexity of the institution rather than asset size. Notably, each institution that completed the CAT indicated the first completion took considerably more time than a subsequent update. For example, one institution reported that initially it took 40 hours to complete the CAT; for subsequent evaluations, it only took 1-2 hours to update and on an annual review basis, 15-20 hours.

With regard to start-up costs, they include, but are not limited to, considerations such as time and consultant fees, and range anywhere from $3,000 up to $10,000. Again, most banks reported that the bulk of these fees were incurred at the initial completion of the CAT and that consultants were not needed for subsequent iterations.

Automation

The notice and request for comments asks for ways to minimize the burden of the collection on respondents, including through the use of automated collection techniques or other forms of information technology. None of the banks responded favorably to automated collection of CAT information by the agencies. In fact, several banks were concerned that automated collection would lead to a greater need to provide defensible answers during the examination review of the CAT. Many banks find it useful to discuss the CAT with the examiner on-site.

ICBA appreciates the opportunity to share the views of our members with the agencies about the CAT. Should you have any questions or would like to further engage on these or other cybersecurity topics, please reach out to me at Jeremy.Dalpiaz@icba.org or by phone at 202-659-8111.

Respectfully Submitted,

/s/
Jeremy J. Dalpiaz
Vice President, Cyber and Data Security Policy