



Brad M. Bolton, *Chairman*
Derek B. Williams, *Chairman-Elect*
Lucas White, *Vice Chairman*
Tim R. Aiken, *Treasurer*
Sarah Getzlaff, *Secretary*
Robert M. Fisher, *Immediate Past Chairman*
Rebecca Romero Rainey, *President and CEO*

July 22, 2022

Via Electronic Submission

Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency
Attention: 1557-0328
400 7th Street SW, Suite 3E-218
Washington, DC 20219

RE: FFIEC Cybersecurity Assessment Tool—OMB Number: 1557-0328

On behalf of the Independent Community Bankers of America ("ICBA"),¹ we appreciate the opportunity to provide information to the Office of the Comptroller of the Currency ("OCC") who is collecting information on behalf of itself, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the National Credit Union Administration (collectively, the "Agencies") on the Federal Financial Institutions Examination Council Cybersecurity Assessment Tool ("CAT"). Community banks take protecting customer information and their own systems and processes against cyber threats very seriously. ICBA appreciates the OCC's request for comment and its willingness to review the effectiveness of the CAT to improve the tool for community bankers and the Agencies.

¹ *The Independent Community Bankers of America® creates and promotes an environment where community banks flourish. ICBA is dedicated exclusively to representing the interests of the community banking industry and its membership through effective advocacy, best-in-class education, and high-quality products and services.*

With nearly 50,000 locations nationwide, community banks constitute roughly 99 percent of all banks, employ nearly 700,000 Americans and are the only physical banking presence in one in three U.S. counties. Holding nearly \$5.9 trillion in assets, over \$4.9 trillion in deposits, and more than \$3.5 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.

The Nation's Voice for Community Banks.®

WASHINGTON, DC
1615 L Street NW
Suite 900
Washington, DC 20036

SAUK CENTRE, MN
518 Lincoln Road
P.O. Box 267
Sauk Centre, MN 56378

866-843-4222
www.icba.org

Recommendations

ICBA frequently engages its members to explore how community banks utilize different technologies and frameworks to keep customer information and bank data safe. The following reflects their comments about the use and functionality of the CAT. ICBA encourages the Agencies to consider the following:

1. The use of the CAT by financial institutions should remain voluntary.
2. Establish a working group of public and private sector participants to complete regular reviews of the CAT.
3. Create resources for bank leadership to further educate them on the CAT.
4. Provide community banks access to trending information and statistical analysis.

Voluntary Assessment Tools

ICBA agrees with the Agencies' position that the use of the CAT should remain voluntary for financial institutions as outlined in the FFIEC IT Handbook, which provides that institutions can reference one or more recognized technology frameworks.² ICBA supports that community banks should be able to continue to select the risk-based frameworks that best meet community banks' needs, level of complexity, and level of risk.

CAT Maintenance

ICBA agrees with the Agencies that the CAT may provide a useful tool for a community bank to identify its inherent cyber risk profile. Banks can use the CAT's maturity matrix to evaluate cybersecurity preparedness based on their cyber risk management and oversight, threat intelligence and collaboration, cybersecurity controls, external dependency management, and cyber incident management and resiliency planning. A financial institution may use the matrix's maturity levels to identify opportunities for improving its cyber risk management, based on its inherent risk profile. The CAT also enables a financial institution to identify areas that could improve the financial institution's cyber response programs, as appropriate.

While recognizing that a variety of risk-based frameworks are suitable for banks to use, it is important to recognize that the CAT has significant penetration in the financial services sector with 89% of financial institutions utilizing the CAT.³ Community banks and other financial institutions have invested significant time and resources into developing a CAT maturity profile and a risk-based program. Switching to a new framework or tool would introduce additional and unnecessary costs for community banks so it is important that the CAT continue as a tool for community banks, internal and external auditors, and their regulators.

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>

³ Tandem survey. "The State of Cybersecurity in the Financial Institution Industry." 2021. See <https://tandem.app/state-of-cybersecurity-report/download/2021>

It is also important to maintain and keep the CAT up to date to properly reflect the ever-changing risk environment that community banks face. To keep the tool up to date, ICBA suggests that community banks and ICBA have an opportunity to participate in the review process so that the CAT can continue to be improved and right-sized for community banks' needs.

ICBA suggests that as part of a review and improvement process, the CAT be evaluated for opportunities that make the CAT's outputs more understandable to community banks' non-IT senior leadership and board members. This will better raise awareness of cyber risk and remediation activities within financial institutions.

Education of Bank Leadership

To enhance the usefulness of the CAT, ICBA recommends that the Agencies consider creating educational resources targeted to community bank senior leadership and boards of directors. The goal of these resources would be to highlight information from the CAT that would be useful for non-IT senior leaders and board members to review, allowing senior leadership to better understand their bank's risk profile, cyber preparedness, and posture further ensuring appropriate allocation of resources to mitigate vulnerabilities identified therein.

Reporting

ICBA suggests, that if made available to banks, the information collected by the Agencies from the CAT would be useful as means of understanding trends in an emerging threat landscape. Community banks would further benefit from access to sanitized and non-attributable reports and statistical analysis derived from information collected by the Agencies.

CAT and Future Risk Assessment Frameworks

While community banks support and generally rely on the CAT for their risk-based assessments, they have had to expend resources to update their systems or purchase tools from third-party vendors incorporating the CAT framework.⁴ Since banks have an investment in time and money in various finished CAT tools, it would be burdensome and costly to community banks if they were limited to a standardized tool or are required to switch to a different framework.

⁴ Financial Services Sector Coordinating Council. "Automated Cybersecurity Assessment Tool." Accessed 07/19/21. See https://fsscc.org/wp-content/uploads/2021/02/FSSCC_ACAT_v2_1.xlsx

Conclusion

ICBA greatly appreciates the opportunity to provide comments in response to this request and ICBA asks that the Agencies carefully consider our comments and suggestions as they improve the CAT.

If you have any questions, please do not hesitate to contact me at Joel.Williquette@icba.org or (202) 821-4454.

Sincerely,

/s/

Joel Williquette
Senior Vice President, Operational Risk Policy