Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

Executive Summary, 2025-SR-B-008, May 28, 2025

The Board Can Enhance Its Approach to the Cybersecurity Supervision of Community Banking Organizations

Findings

We found that the Board of Governors of the Federal Reserve System can enhance its approach to the cybersecurity supervision of community banking organizations (CBOs). Specifically, we found that the Information Technology Risk Examination (InTREx) work programs are not up to date and do not reflect the evolving information technology (IT) and cybersecurity risk environment. While the interagency nature of InTREx promotes a consistent approach among participating bank supervisors, Board and Federal Reserve Bank interviewees stated that it may limit the Board's ability to update the work programs in a timely manner. Nevertheless, we noted that the Board has customized some of its expectations for IT examinations of CBOs. We believe that the evolving cybersecurity risk environment heightens the need to more timely update the InTREx work programs and the Board's CBO IT supervision approach.

We also found that the selected Federal Reserve Banks' approaches to CBO IT training vary and that the Federal Reserve System does not provide clear training expectations for generalist examiners assigned to conduct CBO IT examinations. While the IT Supervision Network serves as a forum to coordinate IT supervision initiatives, there is no clear accountability for defining System CBO IT and cybersecurity training requirements. We believe that clarifying accountability for Systemwide CBO IT and cybersecurity training and developing a more structured approach to such training can help enhance generalist examiners' preparedness to perform CBO IT supervision.

In addition, we found that the Reserve Banks we reviewed had varying practices for completing and retaining IT Profile (ITP) documents, which examiners use to assess the technology risk of institutions and scope CBO IT examinations. Specifically, the timing for when the selected Reserve Banks completed the ITPs varied. Further, while examiners documented the ITP scores and risk levels in examination scoping workpapers, they did not always retain completed ITPs in the system of record. The Board's 2019 internal guidance does not indicate how to update or whether to retain ITPs. We believe that revising the guidance to address updating and retaining ITPs would promote a more thorough and consistent approach to scoping CBO IT examinations.

Recommendations

Our report contains five recommendations designed to enhance the Board's approach to its cybersecurity supervision of CBOs. In its response to our draft report, the Board concurs with our recommendations and outlines actions to address each recommendation. We will follow up to ensure that the recommendations are fully addressed.

Purpose

We conducted this evaluation to assess the effectiveness of the Board's and the Reserve Banks' cybersecurity supervision approach for CBOs. Specifically, we reviewed the IT and cybersecurity supervision activities of three Reserve Banks—the Federal Reserve Banks of Chicago, Kansas City, and St. Louis—which are overseen by the Board's Division of Supervision and Regulation.

Background

Cyber threats are continually evolving and becoming more complex. *Cybersecurity*—the process of protecting information by preventing, detecting, and responding to attacks—is essential to maintaining the ability to provide financial services to customers. The Board and the Reserve Banks assess CBOs' cybersecurity as part of their IT supervisory activities.

Reserve Banks follow a risk-focused approach and use InTREx to assess CBOs' ability to identify and address IT and cybersecurity risks. InTREx was developed by multiple agencies and is a collection of procedures to help examiners complete IT examinations.