Evaluation Report
2025-SR-B-008
May 28, 2025

Board of Governors of the Federal Reserve System

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

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

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.

Recommendations, 2025-SR-B-008, May 28, 2025

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

Finding 1: The Board Should More Timely Update Its IT Examination Approach for CBOs to Better Reflect Evolving Risks

Number	Recommendation	Responsible office
1	Assess whether the ITP and InTREx work programs used by Reserve Bank examiners address emerging IT and cybersecurity risks and, based on this assessment, provide supplemental guidance and customize the ITP and InTREx work programs for System-led examinations as needed.	Division of Supervision and Regulation
2	Establish a process to periodically assess whether the ITP and InTREx work programs used by Reserve Bank examiners, including the Board's customized guidance, address current material risks in the IT and cybersecurity environment and update the ITP and InTREx work programs as needed.	Division of Supervision and Regulation

Finding 2: The Board Should Develop Formal Guidance on Aspects of Its IT and Cybersecurity Training for CBO IT Examinations

Number	Recommendation	Responsible office
3	Clarify accountability for defining Systemwide CBO IT and cybersecurity training requirements.	Division of Supervision and Regulation
4	Develop IT and cybersecurity training guidance that describes expectations for generalist examiners conducting CBO IT examinations, including expectations for on-the-job training and expectations following the completion of the CBO ECP.	Division of Supervision and Regulation

Finding 3: The Board Should Ensure That Examiners Complete ITPs in a Consistent Manner and Retain Records of Completed ITPs

Number	Recommendation	Responsible office
5	Clarify in guidance the expectations for updating and reaffirming responses in ITPs and retaining ITPs for each IT examination in the appropriate system of record, and expectations for assessing ongoing compliance.	Division of Supervision and Regulation

Contents

Introduction

Objective

Our objective for this evaluation was to assess the effectiveness of the Board of Governors of the Federal Reserve System's and the Federal Reserve Banks' cybersecurity supervision approach for community banking organizations (CBOs). The scope of our evaluation included applicable policies, procedures, and agency practices related to information technology (IT) and cybersecurity supervision of CBOs.[1]

We reviewed the IT and cybersecurity supervision activities conducted by three selected 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 (S&R). Our scope did not include supervisory activities unrelated to IT and cybersecurity. Appendix A describes our scope and methodology in greater detail.

Background

The Board's Role in Supervision

The Board plays a significant role in supervising and regulating financial institutions. Through its oversight, the Board seeks to ensure that the institutions under its supervisory authority operate in a safe and sound manner and comply with laws and regulations. S&R leads the Federal Reserve System's supervisory activities. The division develops and implements policies and guidance for examiners and supervised financial institutions, and it organizes its oversight activities into supervisory portfolios that are generally based on institutions' total asset size.

The CBO portfolio includes domestic banking organizations with less than $10 billion in total assets. Under delegated authority from the Board, Reserve Banks supervise the CBOs in their respective districts. As of June 2024, there were 650 CBOs in the portfolio. Reserve Banks supervise CBOs primarily through point-in-time full-scope safety-and-soundness examinations[2] conducted once every 12 months.[3] Reserve Banks coordinate examinations with the chartering state's bank supervisor and may conduct examinations jointly or alternately with state supervisors.

Cyber Threats Facing CBOs

Cyber threats are continually evolving and becoming more complex as many CBOs adopt more digital solutions and become more reliant on technologies and third parties. Cyberattacks can create substantial operational risk, disrupt critical services, and result in the loss of valuable and sensitive data. According to

[1] Examiners assess cybersecurity during IT examinations, which are conducted in conjunction with safety-and-soundness examinations.

[2] All safety-and-soundness examinations conducted by Reserve Banks include an assessment and evaluation of IT risks and risk management and assign a composite rating under the Uniform Rating System for Information Technology.

[3] Banking organizations with less than $3 billion in total assets that meet certain criteria, such as strong capital positions and satisfactory or better ratings from the most recent examination, may be examined less frequently—once every 18 months.

the Board's November 2024 *Supervision and Regulation Report*, while CBOs have taken steps to strengthen their operations and IT systems, they remain vulnerable to cyber threats.

The CBO Program's Cybersecurity Supervision Approach

Effective IT risk management is critical to the safety and soundness of financial institutions. An important part of IT risk management is *cybersecurity*—the process of protecting information by preventing, detecting, and responding to attacks. Effective cybersecurity helps institutions to maintain the ability to provide financial services to customers. The Board and the Reserve Banks follow a risk-focused approach to assess CBOs' cybersecurity as part of their IT supervisory activities.

Reserve Banks use the Information Technology Risk Examination (InTREx) program to assess institutions' ability to identify and address IT and cybersecurity risks. InTREx is a collection of work programs that help examiners assess institutions' IT risk management and operational areas. The Federal Deposit Insurance Corporation, the Conference of State Bank Supervisors, and the System developed InTREx -- it applies to banks with assets less than $100 billion, including CBOs.[4]

The interagency InTREx Committee consists of members from the Federal Deposit Insurance Corporation, the Conference of State Bank Supervisors, and the System. According to the InTREx Committee charter, the committee ensures that InTREx remains current and releases any updates or revisions to examiners in a timely manner. The charter also states that the committee should review and update the InTREx work programs at least every 3 years.[5]

The Board issued internal guidance in 2019 outlining its InTREx implementation expectations for Reserve Bank examiners, including instructions for applying InTREx procedures. The first step in an IT examination is to assess an institution's technology risk and develop the scope by completing the InTREx Information Technology Profile (ITP). The ITP consists of 13 questions addressing an institution's IT environment, such as core processing, network access and monitoring, and cybersecurity. The Board added 6 questions that cover an institution's patch management and disaster recovery plan as well as findings from the two most recent examinations to help Reserve Bank examiners further focus their examination on risk.

As outlined in the Board's 2019 guidance, an IT examiner in charge (EIC) or central point of contact should review the previous ITP and contact an institution to resolve any information gaps and complete the ITP questions. Based on the answers to the questions, the ITP generates a score that determines one of three risk levels for an institution: *low*, *moderate*, or *high*. Examiners have discretion to make qualitative adjustments to the risk level. An institution's ITP risk level helps examiners determine which InTREx work programs to complete.[6]

---

[4] InTREx also applies to institutions in the Regional Banking Organization portfolio, which includes domestic banking organizations with total assets of $10 billion to $100 billion. In addition, InTREx applies to U.S. branches and agencies of foreign banking organizations with combined U.S. assets of less than $100 billion and certain bank holding companies and saving and loan holding companies with less than $100 billion in total consolidated assets.

[5] The interagency committee updated its charter in August 2023 to state that the committee should review and update the InTREx work programs at least every 3 years.

[6] In addition to the ITP risk level, an institution's business activities, size, and complexity may influence which InTREx work programs to complete.

- ITP risk score of *low*: For low-risk institutions, Reserve Bank examiners use the Base InTREx work program. The Base InTREx work program contains procedures for each of the four Uniform Rating System for Information Technology (URSIT) components: (1) audit, (2) management, (3) development and acquisition, and (4) support and delivery. Using those procedures, examiners assess an institution's overall condition and assign an URSIT composite rating; they do not issue ratings for each component area.[7]
- ITP risk score of *moderate*: For moderate-risk institutions, examiners complete the core procedures in the InTREx work programs. The core procedures cover the four URSIT component areas, and examiners assign a component rating for each area as well as a composite rating.
- ITP risk score of *high*: For high-risk institutions, examiners use the core procedures in the InTREx work programs and complete additional, more-detailed procedures for each URSIT area to assign an institution the four URSIT component ratings and a composite rating.[8]

Reserve Banks have varying approaches to staffing IT examinations. For example, at one of the Reserve Banks we selected for review, IT specialists conduct all CBO IT examinations. The other two Reserve Banks assign generalist safety-and-soundness examiners to low-risk CBO IT examinations and IT specialists to conduct IT examinations of moderate- and high-risk institutions.

The Information Technology Supervision Network

In 2023, Board and Reserve Bank leadership created the IT Supervision Network (ITSN) to organize and coordinate CBO IT supervision and promote a consistent supervisory approach.[9] The ITSN serves as a forum to develop, implement, and maintain IT supervision initiatives. For example, certain ITSN members participate on the interagency InTREx Committee and contribute to reviewing and updating the InTREx work programs. According to its charter, the ITSN also coordinates with System supervision programs and committees to evaluate IT training and IT staff development for CBO IT supervision.

IT and Cybersecurity Training

The Board and Reserve Banks provide examiners a variety of CBO IT and cybersecurity training courses to prepare them to conduct CBO IT supervisory work. Generalist safety-and-soundness examiners must complete the IT portion of the Board's CBO Examiner Commissioning Program (ECP),[10] which covers IT risks. The System also offers other training options that cover the current InTREx work programs and address topics related to emerging cybersecurity and IT risks at CBOs.

---

[7] The rating scale ranges from 1 to 5, with a rating of 1 indicating the least supervisory concern and a rating of 5 indicating the greatest supervisory concern.

[8] Depending on the institution's size and complexity, examiners may conduct additional procedures, such as the payment systems work program and the InTREx expanded work programs, to further assess the institution's operations. Examiners complete the payment systems work program when the institution meets certain risk criteria, such as contracting with a new payment processing service provider or experiencing a payments-related outage. Examiners may also complete the InTREx expanded work programs to further assess the institution's condition.

[9] The ITSN also covers IT supervision of the Regional Banking Organization portfolio.

[10] The CBO ECP provides examiners with a foundation for supervision in the System and the skills necessary to effectively perform EIC responsibilities at a typical community bank.

Finding 1: The Board Should More Timely Update Its IT Examination Approach for CBOs to Better Reflect Evolving Risks

We determined that the InTREx work programs are not up to date and do not reflect the evolving IT and cybersecurity risk environment. Most InTREx work programs were last updated in either 2019 or 2016 and both updates were less frequent than expected by the interagency InTREx Committee charter. While the interagency nature of InTREx promotes a consistent approach among participating bank supervisors, Board and Reserve Bank interviewees stated that it may limit the Board's ability to update the work programs timely. We noted, however, that the Board has customized some expectations for System-led CBO IT examinations to support risk-focused supervision. In our opinion, the evolving cybersecurity risk environment heightens the need for the Board to more timely update the InTREx work programs and its approach to IT supervision of CBOs. Examiners' use of outdated work programs may hinder the effectiveness of the System's IT examinations.

InTREx Work Programs Are Outdated and Do Not Reflect Emerging IT and Cybersecurity Risks

Even though the Board uses a risk-focused examination approach for CBO IT supervision, we determined that the InTREx work programs have not kept pace with the evolving cybersecurity and IT risk environment. Several examiners stated that the InTREx work programs are effective in guiding examiners through examination procedures. However, several interviewees from the Board and each selected Reserve Bank expressed concerns that the InTREx work programs are not up to date and do not reflect emerging risks in the IT and cybersecurity environment. Our analysis confirmed these views. We found the following:

- The majority of the InTREx work programs were last updated in either 2019 or 2016.[11]
- The InTREx work programs do not cover institutions' use of artificial intelligence.[12]
- The InTREx work program for assessing an institution's authentication and access to financial institution services and systems had not been updated to reflect the guidance detailed in

[11] The management work program and development and acquisition work program were last updated in 2016. The support and delivery work program, the Base InTREx work program, and payment systems work program were updated in 2019. In addition, the audit work program and corresponding audit sections of the Base InTREx work program were updated in 2023.

[12] As noted in the Board's July 2024 *Cybersecurity and Financial System Resilience Report*, artificial intelligence presents both opportunities and significant threats within the financial sector, and it will be important to mitigate its risks. In addition, in November 2024, the U.S. Department of the Treasury's Financial Crimes Enforcement Network issued an alert to help financial institutions identify fraud schemes associated with the use of artificial intelligence by threat actors, such as the use of deepfake media, which is a type of synthetic content.

Supervision and Regulation Letter (SR Letter) 21-14, *Authentication and Access to Financial Institution Services and Systems*.[13]

The InTREx Committee charter states that the committee's purpose is to ensure that the ITP and the InTREx work programs remain current, effective, risk-focused, and aligned with supervisory guidance, and that any updates and revisions are released for examiners in a timely manner. In August 2023, the committee updated its charter to state that the committee should review and update the InTREx work programs at least every 3 years.

While the interagency nature of InTREx promotes a consistent approach among participating bank supervisors, Board and Reserve Bank interviewees said that it may limit the Board's ability to make timely updates. We noted, however, that the Board has established some customized expectations for System-led CBO IT examinations. For example, the Board customized the ITP by adding 6 questions to supplement the 13 standard ITP questions to better risk-focus CBO IT supervision. In addition, the Board developed its own customized work program for low-risk CBO IT examinations to support risk-focused supervision.

Some Reserve Banks assign generalist examiners to conduct CBO IT examinations for low-risk institutions. Although generalist examiners complete some IT training as part of the CBO ECP, they may rely on the InTREx work programs to guide them through examinations. The evolving nature of IT and cybersecurity risks heightens the need to more timely update the InTREx work programs and the Board's customized guidance. Examiner reliance on outdated work programs may hinder their ability to effectively conduct IT examinations and may result in inaccurate assessments of an institution's risks.

Recommendations

We recommend that the director of S&R

1. Assess whether the ITP and InTREx work programs used by Reserve Bank examiners address emerging IT and cybersecurity risks and, based on this assessment, provide supplemental guidance and customize the ITP and InTREx work programs for System-led examinations as needed.
2. Establish a process to periodically assess whether the ITP and InTREx work programs used by Reserve Bank examiners, including the Board's customized guidance, address current material risks in the IT and cybersecurity environment and update the ITP and InTREx work programs as needed.

Management Response

In response to our draft report, the director of S&R concurs with our recommendations. Regarding recommendation 1, the response states that by September 30, 2026, the Board will utilize IT subject matter experts to assess the ITP and InTREx work programs to determine whether these tools address emerging IT and cybersecurity risks. The response also states that the Board will collaborate with the

[13] The Board's InTREx support and delivery work program cites the Federal Financial Institutions Examination Council guidance, *Authentication in an Internet Banking Environment* (SR Letters 05-19 and 11-9), which SR Letter 21-14 superseded.

interagency InTREx committee where possible, and the System will provide examiners with supplemental guidance and customize the ITP and InTREx work programs as needed.

Regarding recommendation 2, the response states that by September 30, 2026, the Board will establish a process to periodically assess and update the ITP and InTREx work programs to address current material IT and cybersecurity risks.

OIG Comment

The planned actions described by the director of S&R appear to be responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Finding 2: The Board Should Develop Formal Guidance on Aspects of Its IT and Cybersecurity Training for CBO IT Examinations

The Board and the Reserve Banks provide examiners with a variety of CBO IT and cybersecurity training courses, as well as on-the-job training, to prepare them to conduct CBO IT supervisory work. However, we found varied approaches to this training among the selected Reserve Banks. We also found that the System does not provide clear training expectations for generalist examiners conducting CBO IT examinations after they have completed the CBO ECP. We noted that another financial regulator's IT training guide includes a recommended roadmap for IT training. While the ITSN coordinates with System supervision programs and committees for IT training and staff development, there is currently no clear accountability for defining System CBO IT and cybersecurity training requirements. We believe that clarifying accountability for defining Systemwide CBO IT and cybersecurity training requirements and developing a more structured approach to such training can help enhance generalist examiners' preparedness to perform CBO IT supervision.

Reserve Bank Approaches to CBO IT Training Vary

The System provides various IT and cybersecurity training options to examiners who conduct CBO IT examinations. For example, generalist safety-and-soundness examiners must complete the IT portion of the CBO ECP, which includes 46 hours of training on IT risks. The ECP also includes optional on-the-job training repetitions in which generalist examiners participate in CBO IT examinations as trainees. Additionally, the System offers the "CBO Fundamentals of Information Technology" program, which includes case studies on the CBO IT environment and the InTREx work programs. CBO IT training also includes other discretionary training options that address topics related to emerging cybersecurity and IT risks at CBOs.

While CBO examiners have several IT training options, the selected Reserve Banks have varied approaches to CBO IT training. We found that each Reserve Bank develops its own approach to on-the-job training for generalist examiners conducting CBO IT examinations. For example, the number of on-the-job training repetitions that CBO examiners conduct varies among the Reserve Banks. We learned that some CBO examination staff have concerns about the lack of formality and structure of the training programs and expressed a need for additional on-the-job training opportunities to ensure they are trained on each IT component of an examination.

Additionally, we found that the System does not provide clear training expectations for generalist examiners conducting CBO IT examinations after they have completed the CBO ECP. For example, generalist examiners from the three Reserve Banks we selected stated that they took the "CBO Fundamentals of Information Technology" program as part of CBO IT training; however, only one of the three selected Reserve Banks requires its examiners to complete the program.

We noted that another financial regulator provides a roadmap for IT training. The financial regulator's examiner training program includes various IT training courses. In addition, that regulator's IT training guidance includes a recommended training path diagram that depicts the preferred sequencing for various IT courses, ranging from basic to advanced, with required completion time frames for mandatory courses.

As noted earlier, the System created the ITSN to coordinate CBO IT supervision and to promote consistency. According to the ITSN's charter, the ITSN coordinates with System supervision programs and committees to evaluate needs and solutions for IT training and IT staff development. However, there is currently no clear accountability for defining Systemwide CBO IT and cybersecurity training requirements. Additionally, under the CBO ECP, on-the-job IT training is optional. Further, some Reserve Banks assign generalist examiners to conduct IT examinations for low-risk institutions. However, current guidance does not clearly outline IT training expectations for generalist examiners following the completion of the CBO ECP.

Training should accommodate the varied backgrounds and experience levels of examiners conducting CBO IT examinations. We believe that clarifying accountability for defining Systemwide CBO IT and cybersecurity training requirements and developing a more structured approach to CBO IT and cybersecurity training can help enhance generalist examiners' preparedness to perform IT examinations of CBOs throughout the System.

Recommendations

We recommend that the director of S&R

3. Clarify accountability for defining Systemwide CBO IT and cybersecurity training requirements.
4. Develop IT and cybersecurity training guidance that describes expectations for generalist examiners conducting CBO IT examinations, including expectations for on-the-job training and expectations following the completion of the CBO ECP.

Management Response

In response to our draft report, the director of S&R concurs with our recommendations. Regarding recommendation 3, the response states that by December 31, 2026, the Board will identify and formalize accountability for Systemwide IT and cybersecurity training.

Regarding recommendation 4, the response states that by December 31, 2026, the Board will develop IT and cybersecurity training guidance that describes expectations for generalist examiners who conduct CBO IT examinations. The response also states that this guidance will address expectations for on-the-job training and the requirement that an examiner complete the CBO ECP.

OIG Comment

The planned actions described by the director of S&R appear to be responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Finding 3: The Board Should Ensure That Examiners Complete ITPs in a Consistent Manner and Retain Records of Completed ITPs

We found that the selected Reserve Banks had varying practices for completing and retaining ITPs. For example, while examiners documented the ITP scores and risk levels in examination scoping workpapers, we were unable to determine when examiners completed the ITPs for some of the examinations we reviewed because examiners did not retain those ITPs. The Board's 2019 internal guidance provides some expectations for when examiners should update ITPs; however, the guidance does not indicate how to update ITPs or whether to retain them. We believe that revising the guidance to clarify expectations for updating and retaining ITPs will promote a more thorough and consistent approach to scoping CBO IT examinations and help ensure the efficient allocation of examination resources.

Reserve Banks' Practices for Completing and Retaining ITPs Varied

We found that the three Reserve Banks we selected have varying practices for completing and retaining ITPs. Interviewees at two of the Reserve Banks stated that the IT EIC contacts an institution's management several weeks before the examination start date to gather information to complete the ITP. However, at one of these Reserve Banks, we were unable to determine whether examiners completed the ITPs before the examination start date for three of six selected examinations because examiners did not upload the ITPs to Supervision Central.[14] At the second Reserve Bank, the ITPs for three of seven selected examinations were dated more than a year before the examination start date. Although our analysis showed that examiners documented the CBO's ITP scores and risk levels in examination scoping workpapers, examiners did not always reaffirm and document whether the prior ITP responses were still accurate before the current examination.

Interviewees at the third Reserve Bank stated that the Bank's team of IT specialists updates ITPs as new information becomes available, such as from an institution, or based on the results of a state examination report. In addition, interviewees from this Reserve Bank noted that the team reviews the ITPs to ensure the risk scores are appropriate for CBOs within the Reserve Bank's district as part of its annual risk-tiering process. Examiners at this Reserve Bank also update the ITP using information they obtain about an institution while conducting an examination. Examiners use this information to scope an institution's subsequent IT examination.

[14] Supervision Central is a cloud-based application that the System adopted in June 2021 for supervised institutions with less than $100 billion in total assets. It supports collaboration and information sharing among several stakeholders, including Reserve Bank supervision staff, institution staff, and staff at other regulatory agencies. Reserve Bank supervision staff must document their supervisory activities in Supervision Central.

The Board's 2019 internal guidance states that the purpose of the ITP is to assess the technology risk of an institution and to develop the examination scope. According to the guidance, Reserve Banks should update ITPs when examiners become aware of any significant changes that could affect an institution's risk profile and before every examination led by the System. The guidance further states that the IT EIC should contact an institution's management to obtain relevant information to complete the ITP.

While the internal guidance provides some expectations for when examiners should update ITPs, it does not provide clear guidance on how to update ITPs or whether to retain them. For example, the guidance states that the IT EIC or the central point of contact should review the preceding ITP and contact an institution to resolve any information gaps 75 days before the examination start date, but it does not indicate how examiners should reaffirm answers in the preceding ITP.[15] In addition, while the guidance states that an IT EIC should document the examination scope and relevant information to support the scope in the examination workpapers, it does not state whether examiners should retain copies of completed ITPs.

A timely and accurate ITP risk score ensures that IT examination scopes are based on the most up-to-date information and promotes the efficient allocation of resources for CBO IT examinations. Additionally, retaining the ITP for each examination ensures that examiners have access to historical data on an institution. We believe that revising the internal guidance to clarify expectations for updating and retaining the ITPs and assessing compliance with that guidance would promote a more thorough and consistent approach to scoping CBO IT examinations.

Management Actions Taken and OIG Assessment

The Board updated its internal guidance in February 2025, shortly before we issued our discussion draft report to the agency. ITSN members informed us that the Board plans to communicate these updates to examiners and conduct training. Our assessment of the policy is that it does not fully address the guidance deficiencies that we identified. For example, the updated guidance indicates that examiners should document and retain the risk profile with the examination workpapers; however, it does not specifically state whether examiners should retain completed ITPs. We believe the Board can further improve the guidance by explaining how examiners should update and reaffirm responses in the ITPs and by clarifying that examiners should retain ITPs as part of the risk profile in the appropriate system of record.

Recommendation

We recommend that the director of S&R

5. Clarify in guidance the expectations for updating and reaffirming responses in ITPs and retaining ITPs for each IT examination in the appropriate system of record, and expectations for assessing ongoing compliance.

[15] In February 2025, the Board updated its internal guidance to remove the 75-day time frame. The updated guidance states that examiners should update the ITP before developing the examination scope.

Management Response

In response to our draft report, the director of S&R concurs with our recommendation. Regarding recommendation 5, the response states that by September 30, 2026, the Board will update the current internal guidance to clarify expectations regarding the reaffirmation and retention of ITPs. The response also states that before finalizing the guidance, Board staff will assess examination records compliance with existing internal guidance and compliance frameworks.

OIG Comment

The planned actions described by the director of S&R appear to be responsive to our recommendation. We will follow up to ensure that the recommendation is fully addressed.

Appendix A: Scope and Methodology

Our objective for this evaluation was to assess the effectiveness of the Board and Reserve Banks' cybersecurity supervision approach for CBOs. The scope of our evaluation included applicable policies, procedures, and agency practices related to the cybersecurity and IT supervision of CBOs. We reviewed the IT and cybersecurity supervision activities executed by the three Reserve Banks we selected—the Federal Reserve Banks of Chicago, Kansas City, and St. Louis—which S&R oversees.

To accomplish our objective, we reviewed data and judgmentally selected the three Reserve Banks. The Districts of these Reserve Banks had the most CBO IT examinations started from January 2022 through December 2023. We then judgmentally selected 18 CBOs that were examined by these three Reserve Banks during the time period, or 6 CBOs for each of the three Reserve Banks. To select the CBOs, we considered attributes such as examination type (independent or joint), ITP risk score (*low*, *moderate*, or *high*), examination composite rating, and examination component ratings. We also considered the asset size of the institutions to include smaller institutions as well as larger institutions from the CBO portfolio. Our selection resulted in 19 CBO IT examinations because 1 of the CBOs had 2 IT examinations during the time period. We reviewed supervisory information and documents for the 19 selected IT examinations, including ITPs, InTREx work programs, scope documents, examination reports, and other examination-specific information. We cannot generalize the results from our selection across the population of Reserve Banks or CBO IT examinations.

We conducted 28 interviews of Board and Reserve Bank officials and staff to gain their perspectives on the CBO portfolio's IT and cybersecurity supervision activities. Specifically, we interviewed officials and staff from the Board and the three Reserve Banks we selected, the ITSN leadership members, and System representatives to the interagency InTREx Committee.

In addition, we reviewed relevant Board policies and procedures, such as SR Letters, Advisory Letters, and supervision manuals applicable to IT and cybersecurity supervision for CBOs. We also reviewed other relevant documentation, such as CBO IT training program materials. Additionally, we reviewed interagency guidance related to IT and cybersecurity supervision.

We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. We conducted our work from March 2024 through February 2025.

Appendix B: Management Response

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, DC 20551

Mr. Michael VanHuysen
Associate Inspector General for Audits and Evaluations
Office of Inspector General
Board of Governors of The Federal Reserve System
Washington, DC 20551

Dear Mr. VanHuysen,

Thank you for the report issued on May 6, 2025, *The Board Can Enhance Its Approach to the Cybersecurity Supervision of Community Banking Organizations (CBOs)*, prepared by the Office of Inspector General (OIG). We appreciate the OIG's efforts in the evaluation and assessment of the effectiveness of the Board of Governors of the Federal Reserve System's (Board) and the Federal Reserve Banks' (System) cybersecurity supervision approach for CBOs.

The evaluation focused on information technology (IT) and cybersecurity supervision activities conducted by the Reserve Banks. The OIG interviewed staff from the Board and three Reserve Banks and identified three findings and five recommendations. These findings and recommendations addressed ensuring timely updates to the Board's IT examination approach for CBOs; clarifying accountability for defining IT and cybersecurity training requirements; developing formal guidance on aspects of our IT and cybersecurity training for CBO IT examinations; and ensuring that examiners complete IT Profiles (ITPs) consistently and retain completed ITP records.

Below are responses from the Division of Supervision and Regulation (Board S&R) to these recommendations.

Finding 1: The Board should more timely update its IT examination approach for CBOs to better reflect evolving risks.

> **Recommendation 1:** Assess whether the ITP and the Information Technology Risk Examination (InTREx) work programs used by Reserve Bank examiners address emerging IT and cybersecurity risks and, based on this assessment, provide supplemental guidance and customize the ITP and InTREx work programs for System-led examinations as needed.

Recommendation 2: Establish a process to periodically assess whether the ITP and InTREx work programs used by Reserve Bank examiners, including the Board's customized guidance, address current material risks in the IT and cybersecurity environment, and update the ITP and InTREx work programs as needed.

Management Response for Finding 1: Board S&R agrees that the use of outdated work programs may hinder examiners' ability to effectively conduct IT examinations and may result in inaccurate assessments of an institution's risks. Board S&R also appreciates the OIG's acknowledgement that while interagency collaboration promotes a consistent approach among bank supervisors, it may limit Board S&R's ability to update the work programs in a timely manner. Board S&R will continue to collaborate to the extent possible with the interagency InTREx committee while also balancing System needs to address the evolving cybersecurity risk environment.

Response to Recommendation 1: Board S&R will utilize IT subject matter experts to assess the ITP and InTREx work programs to determine whether these tools address emerging IT and cybersecurity risks. Board S&R will also collaborate with the interagency InTREx committee where possible. In addition, the System will provide examiners with supplemental guidance and customize the ITP and InTREx work programs as needed. The expected completion date to address this recommendation is September 30, 2026.

Response to Recommendation 2: Board S&R will establish a process to periodically assess and update the ITP and InTREx work programs to address current material IT and cybersecurity risks. The expected date to address this recommendation is September 30, 2026.

Finding 2: The Board should develop formal guidance on aspects of its IT and cybersecurity training for CBO IT examinations.

Recommendation 3: Clarify accountability for defining Systemwide CBO IT and cybersecurity training requirements.

Recommendation 4: Develop IT and cybersecurity training guidance that describes expectations for generalist examiners conducting CBO IT examinations, including expectations for on-the-job training and expectations following the completion of the CBO examiner commissioning program (ECP).

Management Response for Finding 2: Several formal System organizations and groups, including experienced IT staff at the Reserve Banks, play important roles in providing vital IT and cybersecurity training to examination staff; however, Board S&R agrees that there is an opportunity to clarify accountability for defining Systemwide CBO IT and cybersecurity training requirements. In addition, Board S&R agrees that supervisory guidance for aspects of IT examinations and cybersecurity training on CBO IT examinations should be developed.

Response to Recommendation 3: Board S&R will identify and formalize accountability for Systemwide IT and cybersecurity training and complete this action by December 31, 2026.

Response to Recommendation 4: Board S&R will develop IT and cybersecurity training guidance that describes expectations for generalist examiners who conduct CBO IT examinations. This guidance will address expectations for on-the-job training and the requirement that an examiner complete the CBO ECP. Board S&R will develop and deliver this guidance by December 31, 2026.

Finding 3: The Board should ensure that examiners complete ITPs in a consistent manner and retain records of completed ITPs.

Recommendation 5: Clarify in guidance the expectations for updating and reaffirming responses in ITPs and retaining ITPs for each IT examination in the appropriate system of record and expectations for assessing ongoing compliance.

Management Response for Finding 3: Board S&R agrees that the 2019 internal guidance does not address how to update or where to retain ITPs, which resulted in identified inconsistent practices among Reserve Banks. While ITPs were maintained in a technology solution (i.e., INSite),[1] INSite's functionality did not retain a historical record of examiner updates. Moreover, examiners documented the CBOs' ITP risk profiles within examination scope memorandums and workpapers as required by internal guidance.

Response to Recommendation 5: Board S&R will update the current internal guidance to clarify expectations regarding the reaffirmation and retention of ITPs. Before finalizing the guidance, Board S&R staff will assess examination records compliance with existing internal guidance and compliance frameworks. The results of this assessment will support efforts to update guidance. Board S&R will complete and provide this update to System staff by September 30, 2026.

We value your objective and independent viewpoints and appreciate the professionalism demonstrated by all OIG personnel throughout this audit and your efforts to understand our process.

Sincerely,

MICHAEL GIBSON Digitally signed by MICHAEL GIBSON
Date: 2025.05.16 16:22:45 -04'00'

Michael S. Gibson
Director
Division of Supervision and Regulation

[1] The INSite platform consists of tools used for both the Safety and Soundness and the Consumer Compliance supervision functions and maintains institutions risk profiles.

Abbreviations

CBO	community banking organization
ECP	Examiner Commissioning Program
EIC	examiner in charge
InTREx	Information Technology Risk Examination
IT	information technology
ITP	Information Technology Profile
ITSN	IT Supervision Network
S&R	Division of Supervision and Regulation
SR Letter	Supervision and Regulation letter
URSIT	Uniform Rating System for Information Technology

Contact Information

General

Office of Inspector General
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Center I-2322
Washington, DC 20551

Phone: 202-973-5000
Fax: 202-973-5044

Media and Congressional

OIG.Media@frb.gov

Hotline

Report fraud, waste, and abuse.

Those suspecting possible wrongdoing may contact the OIG Hotline by mail, web form, phone, or fax.

OIG Hotline
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Center I-2322
Washington, DC 20551

Phone: 800-827-3340
Fax: 202-973-5044