The FDIC's Regional Service Provider Examination Program

December 2023 **AEC Memorandum No. 24-01**

Memorandum

Audits, Evaluations, and Cyber

☆☆☆☆☆☆☆☆

NOTICE

Pursuant to Pub. L. 117-263, section 5274, non-governmental organizations and business entities identified in this report have the opportunity to submit a written response for the purpose of clarifying or providing additional context to any specific reference. Comments must be submitted to comments@fdicoig.gov within 30 days of the report publication date as reflected on our public website. Any comments will be appended to this report and posted on our public website. We request that submissions be Section 508 compliant and free from any proprietary or otherwise sensitive information.

Memorandum To: Doreen R. Eberley
Director, Division of Risk Management Supervision

/Signed/
From: Terry L. Gibson
Assistant Inspector General for Audits, Evaluations, and Cyber

Subject: **AEC Memorandum** | The FDIC's Regional Service Provider Examination Program | AEC Memorandum No. 24-01

We have completed our audit of the Federal Deposit Insurance Corporation's (FDIC) Regional Service Provider (RSP) Examination Program. Our objective was to assess the effectiveness of the FDIC's RSP examination program related to third-party risks to financial institutions. During our fieldwork, we interviewed personnel from the Division of Risk Management Supervision (RMS), officials from other Federal Banking Agencies (FBA),[1] and representatives from two financial sector trade associations. In addition, we assessed FDIC RSP examinations for compliance with interagency service provider guidance and conducted a survey of examination staff to obtain their feedback on the service provider examination program.

Overall, we found that the FDIC has not formally established performance goals, metrics, and indicators to measure overall program effectiveness and efficiency. As a result, we were unable to conclude on the program's effectiveness; however, we identified opportunities to improve the RSP examination program.

We conducted this performance audit from May through December 2023 in accordance with Generally Accepted Government Auditing Standards. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Background

Banks routinely rely on third parties for numerous activities, including information technology (IT) services, accounting, compliance, human resources, and loan servicing. Under the Bank Service Company Act (BSCA),[2] the FDIC, FRB, and OCC have the statutory authority to examine third-party entities (or "service providers") that provide technology services[3] to their regulated financial institutions. Specifically, the BSCA states that the services authorized under

[1] Office of the Comptroller of the Currency (OCC) and Federal Reserve Board (FRB).
[2] Bank Service Company Act of 1962, Pub. L. No. 87-856, 12 U.S.C. §§ 1861-67.
[3] Services include check and deposit sorting and posting; computation and posting of interest and other credits and charges; or any other clerical, bookkeeping, accounting, or similar functions performed for a depository institution. The FDIC has interpreted the BSCA to also include call center, credit card payment processing, fund transfer, security monitoring, system development and maintenance, data processing, internet banking, and mobile banking services.

the Act are "…subject to regulation and examination …to the same extent as if such services were being performed by the bank itself on its own premises."[4]

The FDIC conducts examinations of service providers to evaluate their overall risk exposure and risk management performance, and determine the degree of supervisory attention needed to ensure weaknesses are addressed and risks are properly managed by the financial institutions using these service providers. According to FDIC officials, the primary purpose of these examinations is to ensure safe and sound operations at financial institutions by complementing FDIC's IT examinations.[5]

The FDIC performs service provider examinations using two risk tiers: Significant Service Provider (SSP) and RSP. SSPs are large and complex service providers designated for special monitoring and collaborative interagency supervision at the national level. In contrast, RSPs are smaller in size, less complex, and provide services to banks within a local region. The FDIC typically performs RSP examinations jointly with the FRB and OCC and in compliance with interagency guidance established in the Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook and the FBA Administrative Guidelines.

Within the FDIC, RMS is responsible for administering and implementing the FDIC's RSP examination program. Specifically, each RMS supervisory regional office is responsible for managing and performing RSP examinations within their region. In addition, each regional office coordinates with its FRB and OCC counterparts to schedule, staff, and perform RSP examinations.

The conclusion of each RSP examination results in two key deliverables issued to the service provider, the Letter to the Board and the Report of Examination (ROE). The Letter to the Board is a cover letter addressed to the service provider that describes the purpose of the supervisory activity and the assigned FFIEC Uniform Rating System for Information Technology (URSIT) ratings.[6] The ROE includes the examination's findings, recommendations, and the Examination Concerns Requiring Attention (ECRA).[7] Additionally, per implemented guidance, the FDIC and other FBAs provide a copy of the ROE to their regulated financial institutions when service providers are assigned an URSIT composite rating of 4 or 5. The ROEs of service providers with an URSIT composite rating of 1, 2, or 3 are provided to entitled client financial institutions upon their request.[8]

[4] 12 USC § 1867(c).
[5] The FDIC conducts IT examinations under the IT Risk Examination (InTREx) program as part of its risk management examinations. The InTREx program utilizes a risk-based approach to assess IT and cyber risks at financial institutions.
[6] Examiners evaluate and assess the service provider's ability to identify, measure, monitor, and control IT risks within four URSIT component areas: Audit, Development & Acquisition, Management, and Support & Delivery. Based on this analysis, examiners rate each URSIT component area on a scale from 1 ("strong") through 5 ("critically deficient"). Examiners assign an URSIT composite rating, which is based on the overall results of the evaluation and the URSIT component ratings.
[7] ECRAs (formerly Matters Requiring Board Attention) include all significant findings, examination concerns, and recommendations, along with management responses to such concerns that the examiners deemed to be significant.
[8] Entitled client financial institutions are those that have a current contractual relationship with the service provider or demonstrate that they have entered into contracts with the entity at the time of the examination.

Results

The FDIC has not established performance goals, metrics, and indicators to measure overall program effectiveness and efficiency for the RSP examination program. In addition, we identified several opportunities to improve the RSP examination program: (1) monitor ROE distribution timeliness; (2) comply with examination frequency guidelines; (3) provide additional guidance on how to use RSP examinations in support of the InTREx program; and (4) establish a comprehensive inventory of FDIC-supervised bank service providers and the financial institutions serviced.

Absence of Program-Level Performance Goals, Metrics, and Indicators

RMS has not established performance goals, metrics, and indicators to measure the effectiveness of the RSP examination program. When we requested a listing of RSP examination-related performance goals, RMS officials stated that the RSP examination program goals are included in the annual FDIC Performance Goals and highlighted the following three goals:

- **2023**: Publish a Notice of Proposed Rulemaking to update 12 CFR Part 304.3(d), *Notification of Performance of Bank Services*, to improve data regarding bank reliance on third parties, including cloud infrastructure third parties.
- **2022**: Complete a horizontal review of significant service providers to assess operational resilience.
- **2021**: Complete a horizontal review of significant service providers using the Focused Advanced Cyber Threat work program.

However, the 2021 and 2022 goals are related to SSPs. Only the 2023 goal (i.e., update *Notification of Performance of Bank Services*) is related to SSPs and RSPs. Further, the 2023 goal does not directly address the RSP examination program's performance or define metrics to measure results.

While there is no specific requirement, establishing performance goals, metrics, and indicators would allow RMS to define program expectations and measure overall program efficiency and effectiveness. In addition, the U.S. Government Accountability Office Standards for Internal Control in the Federal Government[9] recognizes performance goals and related measures as key components of an effective internal control system.

Lack of Report Distribution Monitoring

In addition to the lack of program-level performance goals noted above, we found that the FDIC did not establish goals and metrics to define and measure the timeliness of RSP ROE distribution. As previously stated, client financial institutions can request a copy of the ROE for service provider examinations with an URSIT composite rating of

[9] GAO, Standards for Internal Control in the Federal Government (Internal Control Standards) (September 2014).

1, 2, or 3. While the FDIC has procedures to process these requests, it does not track or monitor how long it takes to distribute ROEs to financial institutions.

We met with officials from two financial sector trade associations who emphasized the need for timely reports. According to officials at one association, the process to distribute service provider ROEs from request to fulfillment can take up to 6 months. In addition, they have found that these reports are often outdated or no longer useful once received. When we attempted to assess the timeliness of the RSP ROE distribution process, the FDIC was unable to provide relevant data that could be used to measure the time to process requests and distribute ROEs to financial institutions.

According to FDIC officials, the distribution of RSP ROEs is treated as normal correspondence to financial institutions. As a result, the FDIC does not capture related data points or metrics, or monitor the report distribution process. Fulfilling financial institutions' RSP ROE requests in a timely manner would more effectively enable those institutions to use that information and take any necessary risk remediation actions.

Infrequent RSP Examinations

According to the FBA Administrative Guidelines, examination frequency is based on the RSP's Risk Based-Examination Priority Ranking (RB-EPR) and ranges from 24 to 48 months (see **Table 1**). The RB-EPR is assigned by the FBAs and based on the risk that the RSP's business lines, controls, and risk management processes present to their client financial institutions.

Table 1: RSP Examination Frequency by RB-EPR

A (high risk)	24-month cycle
B (medium risk)	36-month cycle
C (low risk)	48-month cycle

Source: FBA Administrative Guidelines

The FDIC has not performed RSP examinations consistent with interagency guidance on examination frequency (see **Table 2**). Specifically, we found that only 18 of 71 (25 percent) RSP examinations conducted by the FDIC as of March 14, 2023 were performed within the frequency guidelines. Conversely, 53 of 71 (75 percent) RSP examinations were not performed within the frequency guidelines. In addition, 10 of 71 (14 percent) examinations were performed more than 3 years past their examination cycle.

Table 2: RSP Examinations Completed by Risk Ranking

Risk Ranking	Completed On-time	Overdue < 1 year	Overdue 1-3 years	Overdue > 3 years	Total RSP Examinations
A	4	1	13	5	23
B	9	7	15	4	35
C	5	3	4	1	13
Total	18	11	32	10	71

Source: OIG analysis of RMS service provider examination data as of March 14, 2023. This table only includes RSPs for which a follow-up examination was conducted.

When we brought these observations to management's attention, RMS officials stated that they do not have dedicated RSP examination staff and rely on the pool of examiners used for risk management and IT examinations to perform RSP examinations. As such, the FDIC prioritizes staff for risk management examinations, which are required under section 10(d) of the Federal Deposit Insurance Act,[10] and assigns resources to RSP examinations based on availability. Unless legislation is amended to require RSP examinations, the FDIC should make efforts to ensure that staff are available and allocated to consistently meet current examination frequency guidance.

Not Leveraging Examination Information for the InTREx Program

We conducted a survey to gauge the usage of service provider examinations in assessing vendor management oversight at financial institutions during InTREx examinations.[11] Based on the results of our survey, additional guidance and training is needed for examiners to effectively leverage service provider examination information[12] in support of InTREx. Specifically, 85 of 163 (52 percent) survey respondents were not aware of how to obtain or access all service provider examination information. For example, respondents expressed that it is difficult to identify whether an examination was performed on a relevant service provider due to the lack of a comprehensive listing of service provider examinations.

Additionally, 100 of 163 (61 percent) respondents stated they had reviewed service provider examination information in support of an IT examination; however, only 37 of 100 (37 percent) reviewed this information regularly, or over 50 percent of the time.

RMS officials acknowledged that additional guidance is needed for examiners to more effectively leverage service provider examinations as part of the InTREx program. During our fieldwork, RMS issued Regional Director Memorandum (RMS RD Memorandum) 2023-017,[13] which updated InTREx procedures and included new guidance for reviewing service provider examinations with an URSIT composite rating of 3, 4, or 5. Specifically, examiners are now directed to review service provider ROEs to identify risks during planning, and in consideration of their assessment of a financial institution's vendor management oversight. In addition, in September 2023, RMS issued RMS RD Memorandum 2023-018,[14] which instructs examiners on identifying service provider examinations with an URSIT composite rating of 3, 4, or 5.

[10] 12 U.S.C. § 1820.
[11] The survey population included risk management examiners assigned the IT Examiner-in-Charge role for IT examinations during the period of January 1, 2022 to December 31, 2022. In addition, the survey population included IT examiners, as of March 28, 2023, and IT examination analysts, as of June 27, 2023, who both lead and support IT examinations. One hundred and sixty-three of 581 FDIC examiners and IT examination support staff responded to the survey, reflecting a 28-percent response rate.
[12] In the survey, service provider information included the assigned URSIT ratings, ECRAs, Enforcement Actions, and the ROE.
[13] RMS RD Memorandum 2023-017, *Information Technology Risk Examination (InTREx) Procedures* (September 2023).
[14] RMS RD Memorandum 2023-018, *Service Provider Examinations with a Composite Rating of 3, 4, or 5* (September 2023).

Lack of Comprehensive Service Provider and Financial Institution Data

During our audit, we identified an opportunity for the FDIC to leverage available service provider information obtained through its InTREx and service provider examination programs. This information could be used to develop a comprehensive inventory of FDIC-supervised bank service providers to improve the FDIC's supervision of financial institutions and the effectiveness of the RSP examination program. For example, the FDIC requires financial institutions to provide a listing of their service providers during each InTREx examination as part of a deliverable known as the *Information Technology Risk Examination Program Products and Services Template*. Since the FDIC already has this information, RMS could identify the service providers for each bank and develop a comprehensive inventory across RMS's portfolio of financial institutions.

In addition, under the BSCA, financial institutions are required to notify their regulators of new contractual relationships within 30 days.[15] These notifications are primarily used to identify service providers for examination but could be further used to ensure the service provider inventory remains current and accurate.

Management also identified opportunities to expand the use of data in improving the RSP examination program. For example, as part of the 2023 FDIC Performance Goals, the FDIC established a performance goal to publish a notice of proposed rulemaking to update BSCA notification guidance. The purpose of this update is to increase the reliability of BSCA notifications, improve consistency among the FBAs, and allow for data aggregation and analysis.

Unreliable Uniform Customer List

Currently, the FDIC relies on service providers to identify their client financial institutions using the Uniform Customer List (UCL).[16] The UCL serves as the primary source of information that FBAs use to ensure ROEs are distributed only to financial institutions entitled to a copy. However, the FDIC found that the UCL was not a reliable source of information.

Specifically, in 2019, the FDIC, FRB, and OCC established a pilot program to distribute service provider ROEs to all client financial institutions regardless of the URSIT composite rating. During the pilot, the FDIC found that service providers did not always accurately identify client financial institutions. As a result, the FDIC ended the pilot program.

Management acknowledged that improvements are needed and is in the process of updating guidance to improve the accuracy and reliability of the UCL. In addition, the FDIC is considering using other data sources (e.g., BSCA notifications) to complement the UCL.

[15] 12 USC § 1867(c)(2).
[16] The UCL is obtained from each supervised service provider and is a list of financial institutions with whom the service provider has entered into a contractual obligation to provide services.

A comprehensive inventory of contracted service providers would enhance the FDIC's ability to identify RSPs for examination and the financial institutions serviced. For example, the FDIC could target its reviews of RSPs based on the concentration of FDIC-supervised institution clients. These enhancements could result in (1) more risk-based reviews and effective examination coverage, (2) improved monitoring of bank risk remediation efforts should a service provider experience a cyber or security incident, and (3) more accurate identification of client financial institutions entitled to an ROE.

The issues outlined in this memorandum underscore the need for improvements to the RSP examination program. Accordingly, we are making the following overarching recommendation:

> **Recommendation**: We recommend the **Director, Division of Risk Management Supervision**, conduct a formal assessment of the Regional Service Provider examination program to establish program-level goals, metrics, and indicators and determine whether additional resources and controls are needed to improve the effectiveness of the program, as identified in this memorandum.

FDIC Comments and OIG Evaluation

The FDIC's Director of RMS provided a written response, dated December 14, 2023, to a draft of this memorandum. The response is presented in its entirety in **Appendix 1**.

In its response, the FDIC concurred with the OIG's recommendation. The FDIC's proposed corrective actions were sufficient to address the intent of the recommendation, and the FDIC plans to complete all corrective actions by December 31, 2024. We consider the recommendation to be resolved.

The recommendation in this memorandum will remain open until we confirm that corrective actions have been completed and the actions are responsive. In confirming that the corrective actions have been taken, we expect the FDIC will make significant changes to improve the effectiveness of the program, as identified in this memorandum. A summary of the FDIC's corrective actions is contained in **Appendix 2**.

Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990
Division of Risk Management Supervision

December 14, 2023

TO: Terry L. Gibson
Assistant Inspector General, Audits, Evaluations, and Cyber
Office of Inspector General

DOREEN EBERLEY Digitally signed by DOREEN EBERLEY Date: 2023.12.14 19:05:22 -05'00'

FROM: Doreen R. Eberley
Director, Division of Risk Management Supervision

SUBJECT: Draft Audits, Evaluations, and Cyber Memorandum
The FDIC's Regional Service Provider Examination Program (No. 2023-002)

The FDIC has completed its review of the Office of Inspector General's (OIG) draft Audits, Evaluations, and Cyber Memorandum *The FDIC's Regional Service Provider Examination Program* (No. 2023-002) issued on November 9, 2023. FDIC management concurs with the report's single recommendation and provides a full response to the audit findings and recommendation below.

The FDIC's Regional Service Provider Examination Program is high quality, produces accurate ratings under the Uniform Rating System for Information Technology, and identifies weaknesses in information technology (IT) risk management. Further, the FDIC holds service providers accountable for addressing those weaknesses.

The draft memorandum recommends improvements in the Regional Service Provider (RSP) examination program such as establishing performance goals, metrics, and indicators to measure overall program effectiveness and efficiency. The FDIC proposes an improvement strategy and provides an estimated completion date for the OIG's recommendation below.

Management Response to the OIG Findings and Recommendation

Findings: The FDIC has not established performance goals, metrics, and indicators to measure overall program effectiveness and efficiency for th**e** Regional Service Provider examination program. In addition, the OIG identified several opportunities to improve the Regional Service Provider examination program: (1) monitor ROE distribution timeliness; (2) comply with examination frequency guidelines; (3) provide additional guidance on how to use Regional Service Provider examinations in support of the InTREx program; and (4) establish a comprehensive inventory of FDIC-supervised bank service providers and the financial institutions serviced.

Recommendation: We recommend the Director, Division of Risk Management Supervision (RMS) conduct a formal assessment of the Regional Service Provider examination program to establish program-level goals, metrics, and indicators and determine whether additional resources and controls are needed to improve the effectiveness of the program, as identified in this advisory memorandum.

Management Decision: Concur

Planned Action: RMS will assemble a working group with representatives from each regional office (either an IT Assistant Regional Director, IT Supervisory Examiner, or IT Examination Specialist) and the IT Supervision Branch to conduct a formal assessment of the Regional Service Provider examination program. The assessment will establish program-level goals, metrics, and indicators and determine whether additional resources and controls are needed to improve the effectiveness of the program.

Estimated Completion Date: December 31, 2024

cc: E. Marshall Gentry, Chief Risk Officer
John F. Vogel, Deputy Director and Chief of Staff, RMS
Lisa D. Arquette, Deputy Director, RMS
William H. Henley Jr, Associate Director, RMS

Appendix 2 Summary of the FDIC's Corrective Actions

This table presents management's response to the recommendation in the report and the status of the recommendation as of the date of report issuance.

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The RMS Director will assemble a working group with representatives from each regional office to conduct a formal assessment of the Regional Service Provider Examination program. The assessment will establish program-level goals, metrics, and indicators, and determine whether additional resources and controls are needed to improve the effectiveness of the program.	December 31, 2024	$0	Yes	Open

[a] Recommendations are resolved when —

1. Management concurs with the recommendation, and the OIG agrees the planned corrective action is consistent with the recommendation.
2. Management does not concur or partially concurs with the recommendation, but the OIG agrees that the proposed corrective action meets the intent of the recommendation.
3. For recommendations that include monetary benefits, management agrees to the full amount of OIG monetary benefits or provides an alternative amount and the OIG agrees with that amount.

[b] Recommendations will be closed when the OIG confirms that corrective actions have been completed and are responsive.

Federal Deposit Insurance Corporation
Office of Inspector General

3501 Fairfax Drive
Room VS-E-9068
Arlington, VA 22226

(703) 562-2035

★★★★★★

The OIG's mission is to prevent, deter, and detect waste, fraud, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the agency.

To report allegations of waste, fraud, abuse, or misconduct regarding FDIC programs, employees, contractors, or contracts, please contact us via our Hotline or call 1-800-964-FDIC.