FDIC Office of Inspector General

Significant Service Provider Examination Program

Office of Audits

August 2025 | MEMO-25-03

Office of Inspector General

Integrity • Independence • Accuracy • Objectivity • Accountability

☆☆☆☆☆☆☆☆

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.

Date: August 12, 2025

Memorandum To: Ryan Billingsley
Acting Director, Division of Risk Management Supervision

/S/

From: Matthew Simber
Acting Assistant Inspector General for Audits

Subject: Significant Service Provider Examination Program | MEMO-25-03

This memorandum presents the results of our audit of the Federal Deposit Insurance Corporation's (FDIC) Significant Service Provider (SSP) Examination Program. Our objective was to determine the effectiveness of the SSP Examination Program in evaluating the risk exposure and risk management performance of SSPs and determining the degree of supervisory attention needed to ensure weaknesses are addressed and risks are properly managed.

During our fieldwork, we analyzed and reviewed policies, procedures, and other key documents related to the administration of the FDIC's Service Provider Examination Programs. We also interviewed FDIC 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 leveraged Government Accountability Office (GAO) reports to identify leading practices for performance goals and metrics.

We conducted this performance audit from August 2024 through May 2025 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.

In conducting this audit, we obtained an understanding of internal controls necessary to meet the audit objective. Our audit procedures addressed these controls. We also assessed the reliability of data relevant to our audit objective and confirmed the data was sufficiently reliable. Because our review of internal controls was limited, we may not have identified all control deficiencies that may have existed at the time of our audit.

[1] Office of the Comptroller of the Currency (OCC) and the Board of Governors of the Federal Reserve System (FRB).

BACKGROUND

Under the Bank Service Company Act of 1962 (BSCA),[2] the FDIC, FRB, and OCC have the statutory authority to examine covered services provided by third parties to their regulated financial institutions.[3] Specifically, the BSCA states that the services authorized under 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 these examinations to evaluate the 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 financial institutions using service providers. The FDIC typically performs SSP examinations jointly with the FRB and OCC and in compliance with interagency guidance established in the Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook and the FBA Administrative Guidelines. According to FDIC officials, the primary purpose of these examinations is to help ensure safe and sound operations at financial institutions by complementing the FDIC's IT examinations.[5]

Significant Service Providers and Regional Service Providers

The FDIC performs service provider examinations using two risk designations: significant and regional. SSPs are large and complex service providers designated as agreed upon by the FBAs for special monitoring and collaborative interagency supervision at the national level. In contrast, regional service providers (RSP) are smaller in size, less complex, and provide services to banks within a local region. FDIC officials stated that the distinction between SSPs and RSPs is not a statutory definition and that SSPs and RSPs are examined under the same program. However, separating firms using SSP and RSP designations provides administrative benefits due to differences in how firms under each risk designation are examined.[6]

The service providers included in the SSP portfolio evolve over time based on the FBAs' assessment of risk. The FBAs generally have discretion about which and how many service providers to examine. Recent examinations have been performed on those providing core banking, payment processing, cloud service, and other technology services. The FBAs consider quantitative factors such as the number of banking customers the service provider serves, the

---

[2] Bank Service Company Act of 1962, Pub. L. No. 87-856, 76 Stat. 1132, codified at 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.
[4] 12 USC § 1867(c)(1).
[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] Differences between SSP and RSP examinations include SSP examinations are conducted continuously while RSP examinations are more of a point in time; the SSP examinations are performed annually while the RSP examinations can occur every 24 to 48 months or longer; and strategy determinations for SSPs are generally made in the FBAs' national offices while RSPs are managed regionally.

value of the assets held by client banks, and the volume of payments processed in determining which firms to include in the SSP portfolio. There is significant variation in ranges for these metrics. For example, the number of banking customers an SSP provides services to can be as low as 10 or can exceed 4,200.

Since 2020, the FBAs have performed SSP examinations on 16 distinct service providers, 9 of which were examined every year between 2020 and 2023. All 16 service providers were examined at least twice during that window with two additional service providers being examined every year between 2021 and 2023. In addition to the 12-15 annual SSP examinations, FBAs performed approximately 118 RSP examinations during that time. As shown in Table 1, on average, the FBAs performed about 14 SSP examinations and 30 RSP examinations per year for the period 2020 through 2023.

Table 1: Service Provider Examinations From 2020 to 2023

Year	Regional Service Providers	Significant Service Providers	Total
2020	27	14	41
2021	29	14	43
2022	31	15	46
2023	31	12	43
Total	**118**	**55**	**173**

Source: RMS data provided in December 2024.

Absence of Program-Level Goals, Metrics, and Indicators

In December 2023, the OIG issued a memorandum where we found that the FDIC had not established performance goals, metrics, and indicators to measure overall program effectiveness and efficiency for the RSP Examination Program.[7] Accordingly, we recommended that the FDIC conduct a formal assessment of the RSP 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.

In April 2025, the FDIC detailed five corrective actions taken, which included assembling a working group to develop examination program recommendations for (1) improving accountability for meeting timelines, (2) clarifying timelines for expected deliverables, (3) developing processes to support adherence to examination frequency guidelines by better identifying past due RSP examinations, (4) using RSP examinations in support of InTREx, and (5) establishing a comprehensive inventory of FDIC-supervised bank service providers and financial institutions serviced. While these were not goals that could be used to clearly define programmatic success, we acknowledge the FDIC's efforts to respond to the intent of the recommendation related to the RSP Examination Program.

[7] FDIC OIG, *The FDIC's Regional Service Provider Examination Program* (AEC Memorandum 24-01) (December 2023).

Reports of Examination

For SSP examinations, the FBAs issue Reports of Examination (ROE) that include findings, recommendations, and the Examination Concerns Requiring Attention (ECRA).[8] ROEs are generally accompanied by a Letter to the Board, which 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.[9] 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 though specific procedures can vary depending on the FBA. The ROEs of service providers with an URSIT composite rating of 1, 2, or 3 are provided to entitled FDIC-supervised client financial institutions upon their request.[10]

RESULTS

The FDIC has not established program-level performance goals and metrics to measure overall SSP Examination Program effectiveness and efficiency. According to GAO, results-oriented organizations set performance goals to clearly define desired outcomes and develop metrics clearly linked to the goals. While the FDIC has taken steps to establish goals and metrics, they were not measurable or directly linked to program success factors. As a result, we were unable to conclude on the program's effectiveness in evaluating the risk exposure and risk management performance of SSPs and determining the degree of supervisory attention needed to ensure weaknesses are addressed and risks are properly managed. However, we identified an opportunity to enhance the FDIC's SSP Examination Program by more clearly defining its program-level goals.

The FDIC Can More Clearly Define the Program-Level Goals of the Service Provider Examination Programs

Although the FDIC has developed strategic objectives and made progress in its performance management efforts, the FDIC has not established program-level performance goals and

[8] 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.
[9] 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.
[10] 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.

metrics to measure overall SSP Examination Program effectiveness and efficiency.[11] FDIC officials stated that program-level goals and metrics related to the SSP Examination Program were established as part of the corrective actions taken to address the recommendation for the RSP Examination Program. New metrics surrounding the timeliness of report distribution and RSP examination cadence, using RSP reports to support InTREx examinations, and establishing a comprehensive inventory of FDIC-supervised bank service providers and financial institutions serviced should allow the FDIC to better manage its examination programs. However, the corrective actions did not establish goals that clearly define programmatic success, nor could they be used to adequately measure the effectiveness of the SSP Examination Program.

According to GAO, results-oriented organizations set performance goals to clearly define desired program outcomes and develop performance metrics that are clearly linked to the performance goals. Program goals communicate what results the agency seeks and allow agencies to assess or demonstrate the degree to which those desired results are achieved. Performance metrics also show the progress the agency is making toward achieving program goals.[12]

While the FDIC's formal goals and metrics related to the SSP Examination Program were lacking, FDIC officials were able to conceptually describe some of the program outcomes they seek to achieve. In our December 2023 memorandum, FDIC officials were cited as stating "the primary purpose of these examinations [of service providers] is to [help] ensure safe and sound operations at financial institutions by complementing FDIC's IT examinations." During this audit, FDIC officials stated that they used a risk-based approach to attempt to direct examination resources to service providers that pose the greatest risk to banks. The risk factor of greatest concern is the risk of a service provider failure causing a failure at one or more banks, but the FDIC considers other risks such as those related to privacy.

RMS stated that they consider quantitative factors to determine which service providers pose the greatest risk to banks. These factors include metrics such as the number of banking customers the service provider serves, the value of the assets held by client banks, the volume of payments processed, and other key business line metrics. RMS stated that they prioritize examining service providers who interact with the most banks and banks who have the most assets. This helps manage risk because a cyber incident at a large technology service provider

---

[11] According to the federal government's Performance Framework, strategic objectives define and advance the long-term objectives, outcomes, and impacts a program hopes to accomplish. Strategic objectives express the results or direction the agency will work to achieve to make progress on its mission and are supported by more specific performance goals and metrics. Strategic Objective 2.1 in the FDIC's 2022-2026 Strategic Plan states that the "FDIC will exercise its statutory authority, in cooperation with other primary federal regulators and state agencies, to promote safe and sound practices at FDIC-insured institutions, including appropriate risk management." Means and strategies under this objective state that "the FDIC, OCC, and FRB conduct IT examinations of third-party technology service providers that provide a range of services to IDIs. As the threat of cyberattacks continues to be prominent, the FDIC engages with other regulators and the private sector to encourage IDIs and service providers to implement strong preventive programs and to exercise and refine protocols for addressing cyber events when preventive programs are overcome."

[12] GAO, *Federal Buildings GSA Should Establish Goals and Performance Measures to Manage the Smart Buildings Program*, GAO-18-200 (Washington, D.C. January 2018).

has the potential to cause contagion within the financial sector, potentially having widespread impact.

RMS also considers qualitative factors in determining prioritization efforts for SSP examinations. For example, RMS considers the mission criticality and substitutability of the services provided and the potential impact that a disruption in the service would have on the client bank. However, it should be noted that RMS stated they seek to avoid taking actions that would shape the bank service provider market or create the perception that the FDIC is endorsing certain service providers. RMS has concerns that doing so could stifle innovation within the financial sector and could increase the concentration risk posed by larger service providers. Additionally, RMS stated that banks are responsible for vendor management and RMS does not want to create the impression that managing vendor risk is a regulator function.

We observed that the vendor selection process in place when we began our review was highly subjective, poorly documented, and would benefit from additional quantitative analysis. The FBAs set out to establish a new FBA Inherent Risk Methodology Analysis (IRMA) that was a risk-based methodology for measuring and risk-ranking service providers. IRMA is designed to (1) prioritize service providers who are currently supervised to determine the appropriate exam frequency and commensurate resourcing, (2) evaluate whether new service providers should be supervised and added to the program, and (3) evaluate whether existing service providers should no longer be supervised and removed from the program.

IRMA is designed to enable the FDIC to consider quantitative and qualitative factors to determine which service providers pose the greatest risk to banks' safety and soundness. Quantitative factors include metrics such as the number of banking customers the service provider serves, the value of the assets held by client banks, the volume of payments processed, and other key business line metrics. Qualitative factors such as service provider's business line, the mission criticality and substitutability of the services provided, and the potential impact that a disruption in the service would have on the client bank should guide the FDIC's prioritization effort once IRMA is implemented.

While these updates should lead to improved decisions about which providers to select for examination since the selection methodology will be more grounded in quantitative analysis, the effort was not complete as of May 2025. Remaining activities for the FBAs include (1) finalizing and approving risk tier definitions, (2) finalizing and approving documentation for IRMA, (3) continuing to gather volumetric data to support IRMA, and (4) refining the overall workflow, particularly for interagency coordination. Until IRMA is completed, the FDIC does not have assurance that the FBAs are focusing limited examination resources on the firms that pose the greatest risk to banks' safety and soundness.

The concepts described above, including updates to the provider selection process, are more consistent with the outcome-based program-level goals we recommended in our previous audit of the RSP Examination Program. However, these concepts have not been established as programmatic goals, do not clearly define the outcomes the FDIC seeks to create or avoid, and are not effectively measured using clear, reliable, and measurable metrics that are clearly linked to the programmatic goals.

In the absence of clear programmatic goals and metrics, the FDIC has limited assurance that the SSP Examination Program is achieving its intended purpose. Developing program-level goals and metrics will allow the FDIC to define programmatic success, measure the effectiveness of the SSP Examination Program, and support the FDIC's efforts to achieve its strategic objectives related to risk management for third-party service providers.

Recommendation 1:

We recommend the **Director, Division of Risk Management Supervision**, complete efforts to develop and implement program-level goals and metrics for both the Regional and Significant Service Provider Examination Programs. This should include finalizing and implementing the Inherent Risk Methodology Analysis.

Update to the Report Distribution Process

In December 2023, we reported that the FDIC did not establish goals and metrics to define and measure the timeliness of RSP ROE distribution. While the FDIC had procedures to process these requests, it did not track or monitor how long it takes to distribute ROEs to financial institutions. We also reported that these ROEs are often outdated or no longer useful once received. During this audit, we met with officials from two financial sector trade associations to determine whether the process has improved. Officials from both associations informed us that financial institutions still struggle to obtain access to ROEs for vendors and ROEs remain untimely and stale when received by the banks.

In April 2025, the OIG received the FDIC's corrective actions to address the recommendation from our December 2023 memorandum on the RSP examination program. One of these five corrective actions included updating guidance for the distribution of service provider ROEs. This new guidance stated that FDIC "regional office staff should strive to complete the request determination and distribution (if applicable) no later than 45 days from receipt." Further, the guidance instructed FDIC regional offices to "record and track each request including the date received, disposition decision, and date transmitted (if applicable)," which should add accountability to the process. As a result, we are not making a recommendation related to report distribution because the FDIC implemented guidance that should address controllable elements of ROE timeliness.

FDIC COMMENTS AND OIG EVALUATION

On July 28, 2025, the FDIC Acting Director, Division of Risk Management Supervision, provided a written response to a draft of this report, which is presented in its entirety in Appendix 1. In its response, the FDIC concurred with our recommendation and plans to complete corrective actions by March 31, 2026. We consider the recommendation to be resolved. The recommendation in this report will remain open until we confirm that corrective actions have been completed, and the actions are responsive. A summary of the FDIC's corrective actions is contained in Appendix 2.

APPENDIX 1: FDIC COMMENTS

Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Division of Risk Management Supervision

DATE: July 28, 2025

TO: Jason Yovich
Acting Assistant Inspector General for Audits
FDIC Office of Inspector General

FROM: Ryan Billingsley
Acting Director, Division of Risk Management Supervision

RYAN BILLINGSLEY Digitally signed by RYAN BILLINGSLEY Date: 2025.07.28 17:54:40 -04'00'

SUBJECT: Management Response to the Draft Audit Report Entitled *Significant Service Provider Examination Program (2024-014)*

The FDIC appreciates the opportunity to review and comment on the subject FDIC Office of Inspector General's (OIG) draft report entitled *Significant Service Provider (SSP) Examination Program (2024-014)* (the "Report"). The stated objective of the audit was to determine the effectiveness of the SSP Examination Program in evaluating the risk exposure and risk management performance of SSPs and determining the degree of supervisory attention needed to ensure weaknesses are addressed and risks are properly managed.

General Comments

The FDIC appreciates the diligence and professionalism of the OIG in evaluating the effectiveness of the SSP program. The overarching goal of the service provider program is to promote safe and sound practices at FDIC insured institutions, by conducting IT examinations of the most critical third-party technology services. We are pleased that the OIG has acknowledged the progress made by the FDIC and other Federal Banking Agencies (FBAs) to develop a risk-based methodology to help ensure we are achieving this programmatic goal. To that end, the FDIC is eager to formalize our performance goals and metrics to further support the SSP Program.

Recommendations

The Report contains one recommendation.

Recommendation 1: We recommend the Director, Division of Risk Management Supervision, complete efforts to develop and implement program-level goals and metrics for both the Regional and Significant Service Provider Examination Programs. This should include finalizing and implementing IRMA.

Management Response: The FDIC concurs with this recommendation. The FDIC will complete efforts to develop and implement performance goals and metrics for the Regional and Significant Service Provider Program. Additionally, the FDIC will continue to collaborate with the FBAs to advance the Service Provider Criteria Framework, also known as the Inherent Risk Methodology Analysis (IRMA). The IRMA is a risk-based methodology to help ensure we focus on the most critical third-party technology services. It will be an iterative process to finalize this interagency effort. Therefore, for purposes of this recommendation, the FDIC will consider the IRMA finalized once it has been adopted and operationalized for use in FDIC's service provider program.

Estimated Completion Date: March 31, 2026

Thank you for your efforts and if you have any questions or need additional information, please do not hesitate to contact me.

APPENDIX 2: SUMMARY OF THE FDIC'S CORRECTIVE ACTIONS

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

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The FDIC plans to develop and implement performance goals and metrics for the Regional and Significant Service Provider Programs. Additionally, the FDIC plans to continue to collaborate with the FBAs to advance the Service Provider Criteria Framework, IRMA. The FDIC intends to consider the IRMA finalized once it has been adopted and operationalized for use in the FDIC's service provider program.	March 31, 2026	No	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.

FDIC OIG website | www.fdicoig.gov
X | @FDIC_OIG
Oversight.gov | www.oversight.gov