Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation

March 2025

Federal Deposit Insurance Corporation
Office of Inspector General

NOTICE

Pursuant to Pub. L. 117-263, section 5274, non-governmental organizations and business entities identified in this OIG Top Management and Performance Challenges 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: March 14, 2025

Memorandum To: Board of Directors

/S/

From: Jennifer L. Fain
Inspector General

Subject Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation

The Federal Government is undergoing significant restructuring and reform that continues to unfold as we complete our annual assessment of the Top Management and Performance Challenges facing the Federal Deposit Insurance Corporation (FDIC). By statute, the FDIC Office of Inspector General (OIG) is required to include this assessment in the FDIC's Annual Report.

The pace of change and fluidity regarding the status and composition of the FDIC make it difficult to assess the full impact of these changes on the FDIC and its mission. The Top Challenges that we identify below are based on the status, makeup, and processes in place at the FDIC as of March 14, 2025. We acknowledge that the FDIC may undergo significant changes that may impact our currently identified Top Challenges.

We identified eight Top Challenges facing the FDIC:

1. Enhancing Governance
2. Establishing Effective Human Capital Management
3. Ensuring Readiness to Execute Resolution and Receivership Responsibilities
4. Identifying and Addressing Emerging Financial Sector Risks
5. Assessing Operational Resilience in the Financial Sector
6. Improving Contract Management
7. Ensuring IT Security and Scalability
8. Guarding Against Harmful Scams

While these Top Challenges are not rank ordered, we believe that enhancing FDIC governance is critical to ensure that FDIC Divisions and Offices work together to address all identified Top Challenges.

The FDIC OIG will continue to provide independent oversight and serve the American people by preventing, deterring, and detecting waste, fraud, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness.

We are unwavering in our commitment to deliver credible results that drive meaningful change, enhance integrity and accountability, and foster public trust in the FDIC.

Enhancing Governance

Federal agencies and departments are undergoing significant restructuring and reform. The Administration has issued a series of executive orders and other directives with the primary aim to reduce government size and scope in furtherance of workforce optimization. As such, the contours of changes to the FDIC remain unclear. Two of the five seats of the Board of Directors were vacant, with the position of the Chairman being filled on an acting basis by the FDIC's Vice Chairman at the time of this Top Performance and Management Challenges report.[1]

Effective governance of the FDIC by its Board of Directors and senior leaders is critical to ensure that the FDIC can fulfill its mission to maintain stability and public confidence in the Nation's financial system. Elements of a sound governance framework include establishing a culture of high integrity and ethical values;[2] implementing Enterprise Risk Management (ERM) and internal controls to consider and address risks holistically across an organization;[3] as well as measuring progress towards achievement of short- and long-term organizational and program goals.[4]

As noted below, in prior years we have found that FDIC Divisions and Offices tend to work in a siloed, independent fashion rather than as a cohesive enterprise to assess and address risks faced by the FDIC and ensure coordination of activities across FDIC Divisions and Offices. These coordination gaps have impacted the FDIC's mission and programs. We also identified that some FDIC programs either lacked performance goals and metrics, or despite having them, these goals and metrics did not provide a clear measurement of program effectiveness or status.

Fostering Agency-wide Coordination to Work as One-FDIC

ERM is a key governance tool to promote coordination within an agency by allowing leaders to consider and address risks holistically across an agency when developing the agency's strategic plan and budget. The FDIC has established an ERM program, and the FDIC's Operating Committee[5] serves as its governing body and the focal point for the coordination of risk management at the FDIC. The FDIC also has a Chief

---

[1] The FDIC is managed by a five-member Board of Directors that includes a Chairman, a Vice Chairman, the Comptroller of the Currency, the Director of the Bureau of Consumer Financial Protection, and an appointive Director. No more than three members of the Board can belong to the same political party.

[2] According to the Government Accountability Office's Federal Internal Control Standards, an organization's oversight bodies and management should demonstrate a commitment to integrity and ethical values through their directives, attitudes and behaviors, development of standards of conduct to communicate expectations and values, and processes to evaluate adherence to standards and to address any deviations.

[3] OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Controls, states that "Enterprise Risk Management (ERM) and Internal Controls are components of a governance framework." ERM is defined as "a discipline [that] deals with identifying, assessing, and managing risks."

[4] The Government Performance and Results Act (GPRA) requires Federal executive agencies to complete strategic plans; define their missions; establish results-oriented goals and identify the strategies that will be needed to achieve those goals; measure performance toward the achievement of the goals in an annual performance plan; and report annually on their progress in program performance reports.

[5] The Operating Committee is comprised of Division and Office Directors and Deputies to the Chairman.

Risk Officer; however, FDIC Divisions and Offices "[r]etain first-line responsibility and ownership for risk identification, assessment, escalation, management, monitoring, mitigation, and information sharing."[6]

The FDIC has identified interdivisional coordination and information sharing as elevated risks in its ERM Risk Profile since 2020. Also, we continue to find examples where the lack of FDIC internal coordination has impacted the FDIC mission and functions:

- **Preparing for Large Bank Failures.** In our evaluation, FDIC Readiness to Resolve Large Regional Banks (December 2024), we found that FDIC Divisions did not coordinate effectively to ensure that all resolution-related systems were adequate for a large bank resolution and that existing processes for securing a failed bank's information technology (IT) environment were sufficiently scalable. In addition, the FDIC had not completed an Agency-wide staffing analysis to identify a baseline level of FDIC and contractor resources that may be needed for a large regional bank resolution. We also found that the FDIC did not coordinate effectively across Divisions and Offices with key roles for large regional bank resolutions. As a result, risks to important cross-divisional program operations and mission-support functions were not highlighted, discussed, and addressed at the enterprise level.

- **Developing a New Acquisition System**. In our evaluation, The FDIC's Purchase and Deployment of the FDIC Acquisition Management System (FAMS) (January 2024), we found that within 5 months of deployment, the FDIC abandoned a nearly $10 million enterprise-wide acquisition management system and had to revert to its legacy acquisition systems and manual reporting of some acquisition activities. The deployment was unsuccessful because the FDIC did not involve key stakeholders in the purchase and implementation of FAMS. For example, the FDIC Controller was not included in FAMS acquisition planning or the FAMS project steering committee despite having responsibility for the FDIC's financial system, which was to have automated and integrated real-time exchange of data with FAMS.

- **Monitoring for Conflicts of Interest.** In our report, Conflicts of Interest in the Acquisition Process (September 2024), we found that the FDIC does not use financial disclosure information collected by the FDIC's Legal Division to assess individuals for conflicts of interest in contracting. As a result, the FDIC relies on employees to self-identify conflicts of interest. The Office of Inspector General (OIG) established that an FDIC employee serving as a contract Technical Monitor used their official position to assist an adult family member in securing employment with an FDIC contractor and accepted a gift from the employees of the contractor (a prohibited source).

- **Sexual Harassment Reporting and Investigation.** In our report, The FDIC's Sexual Harassment Prevention Program (July 2024), we found that the four FDIC groups charged with implementing the FDIC's anti-sexual harassment program did not act in concert, or share important information, to efficiently and effectively implement the program. This lack of coordinated and effective effort created gaps in accountability for ensuring the anti-sexual harassment program would be implemented in a manner to achieve its objectives.

Measuring Progress Towards Mission Goals

FDIC Board members and senior leaders should also be able to measure achievement of program goals to assess whether programs are on track or require adjustments to staffing, budgets, processes, or other

[6] FDIC Directive 4010.03, Enterprise Risk Management and Internal Control Program.

activities. In our work, we have found examples where FDIC programs either lacked goals and metrics, or existing goals and metrics did not provide a clear measurement of program effectiveness or status.

- **Examining Bank Service Providers.** In our memorandum, The FDIC's Regional Service Provider Examination Program (RSP) (December 2023), we found that the FDIC did not have goals and metrics for its RSP examination program. We found that 75 percent (53 of 71) of bank third-party RSP examinations were not performed within established frequency guidelines, with 26 percent (14 of 53) of these examinations performed more than 3 years past their examination cycle. The delay in RSP examinations was largely due to the FDIC's limited examination staffing, which was deployed to complete statutorily required bank safety and soundness examinations. Absent RSP examinations, the FDIC and banks may not have a full understanding of risks posed by RSPs that may provide IT services, accounting, compliance, human resources, and loan servicing to the bank.

- **Resolving Large Regional Banks.** In our report, FDIC Readiness to Resolve Large Regional Banks (December 2024), we found that the FDIC had established processes to monitor and report performance on Division and Agency-level goals and objectives related to large regional bank resolution readiness activities. However, the FDIC designed these goals and objectives to monitor the progress of specific activities. This method of monitoring did not provide a complete perspective on the FDIC's overall readiness to conduct one or more large regional bank resolutions, and the FDIC had not conducted an overall assessment of its readiness prior to the failures of Silicon Valley Bank, Signature Bank, and First Republic Bank in the Spring of 2023.

- **Preparing for an Orderly Liquidation.** In our report, The FDIC's Orderly Liquidation Authority (OLA) (September 2023), we found that the FDIC had processes to monitor and report performance goals and objectives related to OLA program activities. However, these monitoring and reporting activities did not ensure OLA resolution planning activities had consistently and promptly progressed since the enactment of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act), nor did they provide a clear picture of the overall status of the OLA program or the FDIC's readiness to execute its requirements.

Effective governance allows the FDIC to integrate its Divisions and Offices to ensure that roles, responsibilities, and actions are coordinated and synchronized to address enterprise risks to the FDIC mission. Further, development of effective metrics allows the FDIC Board and senior leaders to understand and measure how FDIC actions and activities progress the FDIC towards programmatic and mission goals and to avoid wasteful spending of the Deposit Insurance Fund (DIF).

Establishing Effective Human Capital Management

Significant changes are underway to reduce the overall size of the Federal Government while maintaining important services to the American people. Federal employees, including FDIC staff, were offered the Deferred Resignation Program (DRP).[7] Further, presidential directives have been issued for agencies to freeze hiring, ensure government functions are aligned with statutory requirements, prepare for large-scale staff reductions, and plan for future hiring at a ratio of one new employee for

[7] Office of Personnel Management (OPM), Fork in the Road: Deferred Resignation Program, https://www.opm.gov/fork (accessed March 3, 2025).

every four departing employees.[8] On February 26, 2025, the Office of Management and Budget and the Office of Personnel Management sent a memorandum to the heads of Executive Departments and Agencies to prepare to initiate a two-phase program for large-scale Reductions-in-Force and reorganization. Under Phase 1, by March 13, 2025, agencies were to submit a plan that focuses on staffing cuts for functions that are not aligned with activities mandated by statute or regulation. In Phase 2, by April 14, 2025, agencies shall propose the future state of their organization, which will be implemented by September 30, 2025.

In previous Top Management and Performance Challenges reports, we identified risks concerning the FDIC's succession management efforts to ensure that mission-critical positions were filled with skilled personnel.[9] As discussed below, we continue to identify this human capital risk. In the near-term, as a result of staff attrition, the FDIC will need to ensure that it has sufficient staff with the necessary skills and qualifications to complete statutorily required examinations and should assess the impact of attrition on the FDIC's capacity to execute resolutions and receiverships effectively.

The full, long-term effect of the restructuring and reshaping of the FDIC is unknown, as these activities are ongoing. In addition to human capital challenges, we also previously identified, and continue to find, that the FDIC has not established an accountable workplace culture, including an adequate sexual harassment prevention program.

Understanding the Impact of Staffing Changes on the FDIC

According to the FDIC, since January of this year, the FDIC has reduced its staffing by approximately 9 percent from over 6,400 permanent and non-permanent employees to less than 5,950. A total of about 453 FDIC employees (approximately 7 percent of all FDIC employees) accepted the DRP offer, and the FDIC dismissed about 162 probationary employees (approximately 2 percent of all FDIC employees). There were also 103 separations—including retirements, resignations, and transfers to other agencies—between January 1 and February 18, 2025, that were unrelated to these activities.

Further, as of February 18, an additional 17 percent of remaining FDIC staff are eligible for retirement in 2025. This includes several senior leaders who will retire within the year such as the Director of the Division of Risk Management Supervision (RMS) as well as Regional Office Directors in the three largest FDIC Regional Offices: Atlanta, Dallas, and New York.

Staff departures can provide opportunities for the FDIC to reshape its business processes and provide opportunities for employee growth; however, there are also near-term risks for the FDIC. With fewer examiners but the same responsibility to conduct statutorily required exams in 2025, it may be difficult for the FDIC to complete these examinations by the end of the year. As a result, the FDIC may need to adjust its current examination processes based on the outflow of skills.

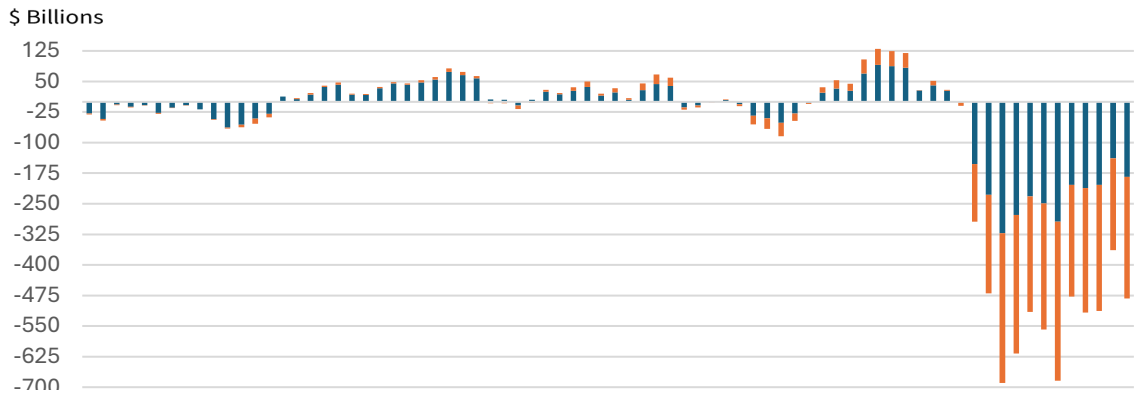
---

[8] Presidential Memorandum, Hiring Freeze, (90 FR 8247) (January 20, 2025); Executive Order 14210, Implementing the President's "Department of Government Efficiency" Workforce Optimization Initiative (90 FR 9669) (February 11, 2025).

[9] Historically, we identified that early career examiners were departing the FDIC at a pace that is greater than retirements for seasoned examiners. As a result, the FDIC faced difficulties maintaining a skilled examination corps to complete statutorily required safety and soundness and consumer protection examinations using current processes and technology. We also noted retirement-eligibility risks for key FDIC Divisions. Although the FDIC had recognized these human capital risks, the FDIC had not developed a successful and coordinated enterprise-wide approach to solving these risks.

Safety and soundness examinations are especially important given potential risks in the banking sector, including with respect to unrealized losses on investment securities. As noted in Figure 1, the FDIC's Quarterly Banking Profile for the 4th quarter 2024 shows unrealized losses on investment securities collectively increased by 32.5 percent from the 3rd quarter. As discussed in the Identifying and Addressing Emerging Financial Sector Risks section of this report, unrealized losses on securities and loans, and concentrations in uninsured deposits contributed to the failure of First Republic Bank.

Figure 1: Unrealized Gains (Losses) on Investment Securities



Source: Statement accompanying FDIC Quarterly Banking Profile, Fourth Quarter 2024. Generally Accepted Accounting Principles state that held-to-maturity (HTM) securities are reported on financial statements at their amortized cost without recognition of any gain or loss. Securities that are available-for-sale are reported at fair value with any gains and losses excluded from net income.

Further, the FDIC will need to assess the impact of staff attrition on its resolution and receivership readiness efforts, including how the attrition may impact the need for contractors. Staff attrition focuses on both the number of departing employees as well as managing the transfer of knowledge and skills. According to the FDIC, as of February 18, 2025, in addition to its 20-percent staff attrition, 25 percent of Division of Resolutions and Receiverships (DRR) remaining staff are retirement eligible within the next year. The Division of Complex Institution Supervision and Resolution (CISR) lost just over 10 percent of its staff with significant losses in its Resolution Readiness Branch. FDIC support divisions for IT, contracting, administrative, financial, and legal services that play an important role during bank failures also faced reductions.

Over the longer term, as the FDIC optimizes its staffing, the FDIC will need to consider, among other things, its investment in new examination staff. It takes about 3 years of training for new examiners to earn an examination commission. Such commissioning requires that employees meet benchmarks, training, and other technical requirements, including passing a Technical Examination. The FDIC will also have to assess its skill composition in response to examiner attrition. In prior Top Management and Performance Challenges reports, we had identified that the FDIC faced risks from departures of examiners, especially those with advanced IT skillsets who examine risks at the most complex banks.

Sustaining a Safe and Accountable Workplace Culture

In our report, The FDIC's Sexual Harassment Prevention Program (July 2024), we found that the FDIC had not implemented an effective sexual harassment prevention program that facilitates the reporting of

misconduct allegations and had not always investigated and addressed allegations of sexual harassment promptly and effectively. This environment of distrust was compounded by the failure of the FDIC to sustain many program improvements that were initiated as a result of recommendations in our report, Preventing and Addressing Sexual Harassment (July 2020).

In our report, Special Inquiry of the FDIC's Workplace Culture (December 2024), we found that a majority of the 2,300 FDIC employee survey respondents stated that they felt safe, valued, and respected and had generally positive views about their coworkers and immediate managers. However, more than one-third of respondents reported that they had either experienced or personally witnessed harassment.[10] Also, FDIC management could not always provide a full account of the surrounding facts related to the disciplinary action taken for harassers, and there was no Agency-wide policy regarding penalties or recommended penalty ranges to ensure the administration of disciplinary and adverse actions is fair and consistent. Further, FDIC policies did not require reporting of allegations of harassment or similar interpersonal misconduct involving FDIC employees to the Chairman or the Board of Directors. As a result, FDIC Senior Executives may not have had sufficient information to understand the extent or significance of the problem across the Agency to take appropriate actions.

With significant staffing changes underway, the FDIC will need to assess its current staff skillsets against its statutory obligations and identify ways to address critical skill gaps. As the FDIC undertakes that assessment, the FDIC should also continue to consider the standards necessary to ensure that the FDIC has an accountable workplace culture.

Ensuring Readiness to Execute Resolution and Receivership Responsibilities

The FDIC is responsible for insuring deposits in our Nation's financial institutions and plays a pivotal role in the resolution and receivership of failed banks.[11] The FDIC is granted resolution and receivership responsibilities under the Federal Deposit Insurance Act (FDI Act) and the Dodd-Frank Act. The FDI Act provides the FDIC with the authority to resolve, and act as receiver for, failed FDIC-insured depository institutions (IDI). The Dodd-Frank Act gives the FDIC Orderly Liquidation Authority to act as a receiver to liquidate failing systemically important financial companies (SIFC) that pose a significant risk to the financial stability of the United States.[12] The FDIC routinely executes its FDI Act receivership powers, but the FDIC has not yet been required to execute its OLA responsibilities.

As described below, we have found that certain aspects of the FDIC's current readiness efforts are not sufficiently mature and require improvement to minimize losses to bank customers and the DIF, and potential costs incurred by other IDIs through special assessments.

---

[10] For these respondents, harassment was in the form of "engaging in bullying, intimidating, or threatening behavior" (64 percent experienced, 67 percent witnessed); "offensive jokes, comments, objects, or pictures" (45 percent experienced, 47 percent witnessed); and "harassment of a sexual nature" (35 percent experienced, 34 percent witnessed).

[11] When a bank fails, the bank is placed in receivership and the FDIC is appointed as its receiver. In general, the term "resolution" refers to the initial phase of a receivership where the FDIC attempts to sell the failed bank to another healthy bank.

[12] A SIFC is any entity that meets the statutory definition of financial company under the Dodd-Frank Act and for which a determination is made that, among other things, the resolution or insolvency of the entity under the otherwise applicable Federal or State law would have serious adverse effects on U.S. financial stability. U.S. organizations that identify SIFCs include the Board of Governors of the Federal Reserve for Bank Holding Companies and the Financial Stability Oversight Council for non-bank financial companies and Financial Market Utilities.

Improving Planning for Large Regional Bank Resolutions and Orderly Liquidations

In our report, FDIC Readiness to Resolve Large Regional Banks (December 2024), we found that the FDIC's readiness to resolve large regional banks was not sufficiently mature at the time of those failures to facilitate consistently efficient response efforts in a potential crisis failure environment. In our report, The FDIC's Orderly Liquidation Authority (September 2023), we concluded that the FDIC had made progress in implementing elements of its OLA program; however, in the 12 years following the Dodd-Frank Act, the FDIC had not maintained a consistent focus on maturing the OLA program and had not fully established key elements to execute its OLA responsibilities. In both reports, we found the following common impediments to FDIC readiness efforts that hinder the FDIC's ability to execute its large regional bank resolution and OLA responsibilities:

- **Lack of Effective Measurement of Readiness Efforts.** In our report, FDIC Readiness to Resolve Large Regional Banks (December 2024), we found that the FDIC had established processes to monitor and report performance on Division and Agency-level goals and objectives to monitor specific large bank readiness activities. However, the FDIC had not measured its overall readiness for large regional bank resolutions. Similarly, in our report, The FDIC's Orderly Liquidation Authority (September 2023), we found that the FDIC did not have adequate monitoring mechanisms in place to ensure it promptly implemented the OLA program and consistently measured, monitored, and reported on the OLA program status and results.

- **Gaps in Information Technology.** In our report, FDIC Readiness to Resolve Large Regional Banks (December 2024), we highlighted that CISR and DRR staff identified 15 significant technology gaps for large regional bank resolutions. For example, existing FDIC processes for securing a failed bank's information technology environment are not sufficiently scalable for a large bank resolution. Although the FDIC had not addressed the overarching technology gaps prior to the bank failures in the Spring 2023, the FDIC stated that it leveraged the failed banks' systems and staff, which minimized some gaps.

- **Absence of Critical Processes and Procedures.** In our report, FDIC Readiness to Resolve Large Regional Banks (December 2024), we found significant missing elements in FDIC resolution procedures. For example, as noted in CISR's process guide, it did not have a receivership expense model to account for reasonable expense estimates for large regional banks or a method for estimating the cost of a bridge bank resolution for least cost test purposes. In our report, The FDIC's Orderly Liquidation Authority (September 2023), we found that the FDIC had not completed process documents and guides to implement CISR's Systemic Resolution Framework and had not adjusted the Framework to facilitate execution of a resolution of systemically important Financial Market Utilities and non-bank financial companies.[13]

- **Unclear FDIC Internal Roles and Responsibilities.** In our report, FDIC Readiness to Resolve Large Regional Banks (December 2024), we found that CISR's large regional bank resolution procedures did not identify and contemplate the key resolution roles that were used in the Spring 2023 failures.

[13] A Financial Market Utility is any person that manages or operates a multilateral system for the purpose of transferring, clearing, or settling payments, securities, or other financial transactions among financial institutions or between financial institutions and the person.

Similarly, in our report, The FDIC's Orderly Liquidation Authority (September 2023), we found that the FDIC had not fully defined governance and individual practitioner-level roles and responsibilities related to the execution of an OLA resolution. Failures may occur quickly, which may not allow the FDIC time to fully define, assign, and train personnel for key governance roles and responsibilities during a resolution.

- **Insufficient Number of Personnel to Execute Readiness Activities Under Current Processes.** In our report on the FDIC Readiness to Resolve Large Regional Banks (December 2024), we found—as shown in Table 1—that since its creation, CISR has had staffing below the levels authorized by the FDIC to achieve readiness efforts. While the FDIC, and CISR in particular, have made large regional bank resolution planning a high priority, the FDIC has not ensured that CISR is able to obtain and retain the human resources that CISR deems necessary to effectively achieve its intended objectives or made changes to processes to require fewer staff. Similarly, in our report, The FDIC's Orderly Liquidation Authority (September 2023), we found that the FDIC had not fully identified and documented the contractor resources necessary for a resolution team to execute an OLA. Further, staffing constraints led the FDIC to shift resources towards large regional bank readiness efforts that otherwise would have been devoted to OLA readiness, which created additional setbacks in maturing the OLA program.

Table 1: CISR Authorized/Actual Positions 2019 - 2023

	2019	2020	2021	2022	2023
CISR – Budget Authorized Positions at Year End	275	273	318	341	369
CISR – Staff on Board at Year End	243	258	280	286	285
Variance	**32**	**15**	**38**	**55**	**84**

Source: OIG Analysis of FDIC Budget Exhibits

The FDIC should stand ready to execute its resolution and receivership powers to maintain financial stability. The FDIC must not lose sight of its readiness mission as it undertakes the restructuring and reshaping of its staff and processes.

Identifying and Addressing Emerging Financial Sector Risks

Currently, the FDIC is the primary Federal regulator for more than 2,800 of the over 4,400 IDIs across the Nation. The FDIC is responsible for examining these IDIs for compliance with safety and soundness requirements, including assessing financial crimes and sanctions risk, and consumer protection requirements. FDIC examinations are key processes to "ensure public confidence in the banking system and to protect the Deposit Insurance Fund."[14] The "accurate identification of existing and emerging risks helps the FDIC develop effective corrective measures for individual institutions and broader supervisory strategies for the industry."[15] In addition to examinations, the FDIC either on its own or in conjunction with other Federal banking regulators provides guidance to banks regarding safety and soundness and consumer protection risks, especially for emerging or novel issues or technology.

[14] The FDIC's Risk Management Examination Manual.
[15] The FDIC's Risk Management Examination Manual.

As discussed below, we have found that the FDIC did not always take early action to mitigate safety and soundness risks identified during bank examinations. We also note that FDIC-supervised banks' increasing use of third-party service providers for compliance with Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) and sanctions requirements may require different examination processes or examiners with different skillsets. Further, although the FDIC and other banking regulators had identified risks with banks' involvement in crypto-asset activities, the FDIC had not conducted risk assessments to determine the significance of crypto-asset activity risks. Moreover, the FDIC's process for providing supervisory feedback to FDIC-supervised institutions' crypto-related activities was unclear.

Escalating Supervisory Actions Through Forward-Looking Supervision and Consideration of Non-Capital Triggers

During the financial crisis of 2008-2011, examiners often identified weak risk management practices at financial institutions but delayed taking supervisory action until the institution's capital declined. Taking supervisory action after a bank's capital has declined is often too late, because financial decline tends to lead to bank failures and losses to the DIF. To avoid that result, the FDIC implemented a forward-looking supervisory initiative to identify and assess risk before it impacts a bank's financial condition and to ensure early risk mitigation.

Section 38 of the FDI Act requires that the Inspector General of the appropriate Federal banking agency conduct a review and issue a written report when there is a material loss to the DIF related to an insured depository institution for which the FDIC is appointed receiver.[16] We conducted three material loss reviews for recent large regional bank failures where we reported that FDIC examiners identified risks at these banks but did not take supervisory action consistent with forward-looking supervision. Our OIG Material Loss Review of Signature Bank of New York (October 2023), and the FDIC Chief Risk Officer's report, FDIC's Supervision of Signature Bank, both found that the FDIC could have escalated supervisory concerns regarding Signature Bank earlier, consistent with the FDIC's forward-looking supervision initiative. These supervisory concerns included multiple opportunities to downgrade the Management component of the bank's CAMELS[17] rating, which may have lowered the bank's composite CAMELS rating and, according to FDIC policy, supported consideration of an enforcement action against Signature Bank.

Similarly, in our report, Material Loss Review of First Republic Bank (November 2023), we reported that the FDIC missed opportunities to take earlier supervisory actions and downgrade First Republic Bank component ratings consistent with the FDIC's forward-looking supervisory approach. Earlier FDIC

[16] FDI Act, Section 38(k), defines the term "material loss" as any estimated loss in excess of "$50,000,000, if the loss occurs on or after January 1, 2014, provided that if the inspector general of a Federal banking agency certifies to the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives that the number of projected failures of depository institutions that would require material loss reviews for the following 12 months will be greater than 30 and would hinder the effectiveness of its oversight functions, then the definition of 'material loss' shall be $75,000,000 for a duration of 1 year from the date of the certification." 12 U.S.C. § 1831o(k).

[17] CAMELS refers to six financial and operational components reviewed in each examination—**C**apital adequacy, **A**sset quality, **M**anagement capabilities, **E**arnings sufficiency, **L**iquidity position, and **S**ensitivity to market risk. Each CAMELS component is assigned a rating on a numerical scale of 1 to 5 based on qualitative analysis. A "1" indicates the strongest performance and management practices and the lowest degree of supervisory concern. A "5" indicates the weakest performance and management practices and the highest degree of supervisory concern. Examiners also assign each bank a composite CAMELS rating based on the agency's evaluation of six component areas. Examiners do not, however, simply assign composite ratings by averaging the individual component ratings. Examiners may give more weight to some components than to others, depending on the perceived risk at a given institution.

supervisory actions may not have prevented First Republic Bank's failure but may have caused First Republic Bank to take corrective action and possibly reduced its susceptibility to contagion risk or reduced the loss to the DIF upon failure.

Further, we noted that the FDIC and other banking regulators should consider adopting non-capital safety and soundness triggers similar to those used for capital ratios.[18] In our report, Material Loss Review of First Republic Bank (November 2023), we noted that the bank was considered well capitalized throughout each examination cycle, so there was no required supervisory action based on capital deterioration. Ultimately, however, First Republic Bank's capital proved insufficient because unrealized fair value losses[19] on securities and loans, and a concentration in uninsured deposits resulted in a final estimated loss to the DIF of $15.6 billion.

Similarly, in our Material Loss Review of Republic First Bank (November 2024) (which is a different institution than First Republic Bank discussed above), we found that the direct cause of the bank's failure was its inability to hold its HTM debt securities to maturity, requiring the securities to be reclassified as AFS. The unrealized losses were disclosed to the public but were not required to be fully reflected in the bank's balance sheet and therefore were not reflected in the bank's capital ratios. Once the losses were fully recognized, all of Republic First Bank's capital ratios immediately fell below zero and the bank was closed. The FDIC was aware of the risks associated with unrealized losses at the bank and within the broader banking industry. In both reports, we recommended that the FDIC engage with other Federal regulators to evaluate the need to identify noncapital triggers that would require early and forceful regulatory actions tied to unsafe banking practices before they impair capital.

In the report, Bank Supervision: Federal Reserve and FDIC Should Address Weaknesses in Their Process for Escalating Supervisory Concerns, the Government Accountability Office (GAO) also found weaknesses in the FDIC's procedures to escalate supervisory concerns to ensure that banks take action. Specifically, the GAO found that the FDIC did not have a centralized system to track recommendations for supervisory actions. Without a tracking system, the FDIC is limited in its ability to identify emerging risks across its supervised banks. Further, the GAO found that unlike other banking regulators, the FDIC does not have vetting meetings "to ensure that large bank examination teams and relevant stakeholders are consulted before making changes or decisions, such as escalation decisions." Finally, the GAO noted that, unlike other banking regulators, the FDIC does not require that large bank case managers rotate to other banks after a few years. GAO noted that these rotations help ensure supervisory independence.

Examining for Financial Crimes and Sanctions Risks

FDIC bank examinations also play a key role to ensure that banks maintain adequate compliance programs to assist U.S. Government agencies in detecting and preventing financial crimes. Such crimes include money laundering, terrorist financing, and other illicit transactions. Federal banking regulators also seek to prohibit domestic banks from conducting transactions with entities sanctioned by the United States through the Department of the Treasury's Office of Foreign Assets Control (OFAC).

---

[18] FDI Act Section 38 mandates that regulators take progressively more severe supervisory actions, known as "prompt corrective actions," as a bank's capital ratio levels deteriorate. FDI Act Section 39 allows regulators to take supervisory action for safety and soundness issues before capital is impaired, but there are no predefined triggers for such actions.

[19] Generally Accepted Accounting Principles state that held-to-maturity (HTM) securities are reported on financial statements at their amortized cost without recognition of any gain or loss. Securities that are available-for-sale (AFS) are reported at fair value with any gains and losses excluded from net income.

Further, the FDIC OIG plays a role in investigating crimes involving FDIC-regulated and insured banks and FDIC activities. Such crimes include, for example, fraud and cyber crimes.

In the July 25, 2024, Joint Statement on Banks' Arrangements with Third Parties to Deliver Bank Deposit Products and Services, banking regulators identified risks to banks resulting from the increasing use of third parties to perform compliance functions such as "monitoring and reporting suspicious activity, customer identification programs, customer due diligence, and sanctions compliance on behalf of the bank. Regardless of whether the functions are shared between the bank and the third party, the bank remains responsible for failure to comply with applicable requirements." Banks' use of third parties for these functions may become more complex when banks rely on a series of third-party relationships.

Banks with ineffective compliance programs or that fail to comply with BSA/AML and OFAC recordkeeping and reporting requirements may face criminal and civil penalties and potentially lose their banking charter. For example, on October 10, 2024, the Department of Justice and our OIG Office of Investigations announced that TD Bank pleaded guilty to BSA and money laundering conspiracy violations and agreed to pay $1.8 billion in penalties. TD Bank failed to maintain an adequate compliance program and "allowed corrupt bank employees to facilitate a criminal network's laundering of tens of millions of dollars."

Bank examinations are an essential element in identifying potential weaknesses in bank BSA/AML and OFAC compliance programs. It is important for the FDIC to ensure that it has examination processes and examiners with the requisite skills to assess financial crimes and sanctions risks posed by banks' third-party affiliations.

Assessing Crypto-Related Activity Risks

In our report, FDIC Strategies Related to Crypto-Asset Risks (October 2023), we found that the FDIC had identified risks with banks' involvement with crypto-related activities; however, the FDIC had not assessed the significance and potential impact of these risks. Specifically, the FDIC had not yet completed a risk assessment to determine whether the Agency could sufficiently address crypto-asset-related risks through actions such as issuing guidance to supervised institutions.

In addition, the FDIC's process for providing supervisory feedback on FDIC-supervised institutions' crypto-related activities is unclear. The FDIC issued letters (pause letters), between March 2022 and May 2023, to certain FDIC-supervised financial institutions asking them to pause, or not expand, planned or ongoing crypto-related activities, and provide additional information. However, the FDIC did not establish an expected timeframe for reviewing information provided and responding to the supervised institutions that received pause letters and describe what constituted the end of the review process for supervised institutions that received a pause letter. In line with the January 23, 2025, Executive Order, Strengthening American Leadership in Digital Financial Technology, the Acting FDIC Chairman stated that the FDIC is "actively reevaluating our supervisory approach to crypto-related activities."[20]

Identification of financial risks as they emerge provides time for banks to take corrective action and for the FDIC to implement supervisory actions such as guidance and enforcement actions, as needed. Prior financial crises have shown that recognition of risk once fully manifested in bank financial statements is generally too late for bank management and FDIC supervisory processes to mitigate such risk.

[20] Statement of Acting Chairman Travis Hill, FDIC Releases Documents Related to Supervision of Crypto-Related Activities (February 5, 2025).

Assessing Operational Resilience in the Financial Sector

Operational resilience refers to "the ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard."[21] Disruptions may result from events such as a cybersecurity incident, technology failures, natural disasters, power grid failures, pandemics, global conflicts, and poor internal controls and risk management. These disruptions may occur at a bank or within the interconnected financial ecosystem of third-party service providers upon which banks increasingly depend. These disruptive events could have multiple impacts, including impeding a bank's ability to deliver services, harming banking systems, and affecting bank data availability and integrity. Disruptive events could erode confidence in the financial sector and cause spill-over events to other financial firms and the broader economy. Further, traditional injections of liquidity and capital to bolster distressed banks are unlikely to solve operational resiliency issues. Operational resiliency requires that banks have well-designed systems, effective risk management and planning, and regular resiliency testing.

As described below, we have found that the FDIC has not conducted bank third-party service provider IT examinations within required timeframes and was not leveraging data from these examinations to understand interconnections across banks and third parties. Further, under current examination processes and considering human capital challenges, the FDIC faces risks that it may not have examiners with appropriate skillsets to effectively assess banks' and third-party operational risks.

Examining for Third-Party Operational Risks

Banks routinely rely on third parties for numerous activities, including IT services, accounting, compliance, human resources, and loan servicing. As noted in the banking regulators' guidance document, Third-Party Risk Management, A Guide for Community Banks, a bank "[e]ngaging a third party does not diminish or remove a bank's responsibility to operate in a safe and sound manner and to comply with applicable legal and regulatory requirements, including consumer protection laws and regulations, just as if the bank were to perform the service or activity itself."

Under the Bank Service Company Act, the FDIC has authority to examine certain services that third parties provide to financial institutions. These examinations complement the FDIC's bank IT examinations. The FDIC performs service provider examinations using two risk tiers: Significant Service Providers (SSP) and Regional Service Providers (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. In our OIG memorandum, The FDIC's Regional Service Provider Examination Program (December 2023), we found that the FDIC had not established performance goals, metrics, and indicators to measure overall RSP examination program effectiveness and efficiency. We also found that:

- **The Frequency of RSP Examinations Was Inconsistent with Guidance.** A total of 75 percent (53 of 71) of RSP examinations completed as of March 2023 were not conducted within guidance

[21] https://www.fdic.gov/news/press-releases/2020/pr20122b.pdf.

timeframes, with 19 percent (10 of 53) of these exams completed more than 3 years past their examination cycle dates. The reason for the delay was because the FDIC lacked examiner resources to conduct these examinations. Without timely RSP examinations, the FDIC is limited in its assessment of banks' current operational risks from these third parties, and banks are not receiving FDIC RSP examination reports that may identify third-party risks.

- **The FDIC Was Not Leveraging RSP Examination Information in Its Bank IT Examinations.** In a survey of 163 IT examiners, we found that 52 percent (85 of 163) of examiners were not aware of how to access RSP examination information. For examiners that did access RSP examination information, only 37 percent said that they did so more than 50 percent of the time. RSP examination information would allow examiners to better understand the risks posed by third parties for the banks that they are examining.

- **Lack of Comprehensive Service Provider and Bank Data.** The FDIC could use information from RSP and bank examinations to develop a comprehensive inventory of service providers and banks. Such a mapping would allow the FDIC to see interconnected risks across a portfolio of banks and third parties rather than on a bank-by-bank basis.

Assessing Banks' Cybersecurity Risks

FDIC bank IT examinations identify areas in which a financial institution is exposed to IT and cyber-related risks and evaluate bank management's ability to identify these risks and maintain appropriate compensating controls. Currently the FDIC faces risks in ensuring that it has examiners with the requisite skillsets to perform IT examinations using existing examination procedures. A total of 53 percent of examiners who are advanced IT subject matter experts were eligible to retire in 2024 with retirement eligibility rising to 63 percent for this population in 2028. Examiners with intermediate IT expertise had retirement eligibility rates of 16 percent in 2024 and 27 percent in 2028. Accurate assessment of IT risks is important as it may affect a bank's safety and soundness rating, which impacts the FDIC's supervisory strategies and may impact the insurance premium paid by a financial institution.

It is critical that the FDIC maps the interconnections of banks and their third parties to understand and examine potential operational points of failure and possible cyber intrusion and contagion. Such maps would also assist the FDIC when assessing resolution risks. Currently, there are instances where multiple banks rely on the same third party. An operational issue at one such third party has the potential to affect many banks. Further, the FDIC should have effective processes and staff with required skillsets to assess operational risks and take supervisory actions as needed.

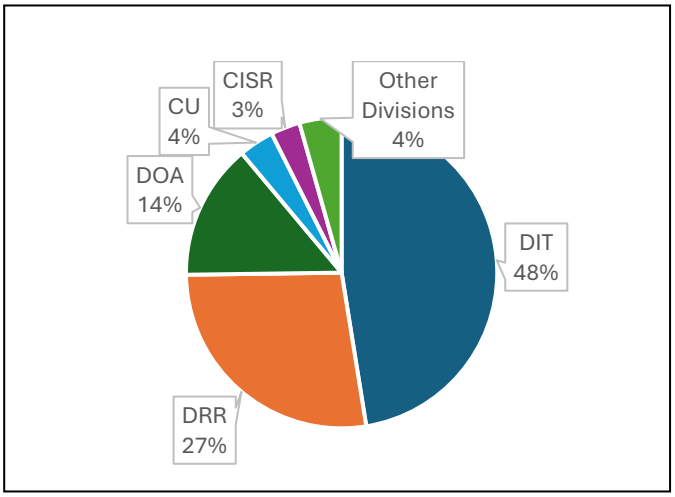
Improving Contract Management

The FDI Act authorizes the FDIC to acquire goods and services to achieve its mission and operations. For the period 2019-2023, the FDIC awarded 2,368 contracts for a total cost of approximately $3.77 billion.

Figure 2 shows the current distribution of contract awards throughout the FDIC.

As discussed below, we continue to identify contract management as a Top Challenge. Our work in this area has identified the need for the FDIC to improve contracting controls and to instill a culture of internal control understanding and compliance. Further, the FDIC should ensure that its contracting personnel are free from conflicts of interest.

Figure 2: Contract Awards Percentage by Division



Source: OIG Analysis of the FDIC's Contracting Dashboard. Division of Information Technology (DIT); Division of Resolutions and Receiverships (DRR); Division of Administration (DOA); Corporate University (CU); Division of Complex Institution Supervision & Resolution (CISR).

Adhering to Contracting Requirements and Internal Controls

In three OIG reports, we have found shortcomings in the FDIC's contract management process and internal controls. These issues have resulted in the FDIC making overpayments, engaging in unauthorized contractual commitments, and abandoning a systems contract. The significance and pervasiveness of identified internal control issues indicate the need for renewed FDIC-wide emphasis on the importance of compliance with internal controls and the stewardship of operating costs incurred by the DIF.

Lack of Coordination and Change Management Resulted in Abandonment of a Nearly $10 Million Investment Towards a New Acquisition System. In our evaluation, The FDIC's Purchase and Deployment of the FDIC Acquisition Management System (FAMS)(January 2024), we found that in June 2022, the FDIC began implementation of its new acquisition system but subsequently abandoned that system within 5 months. As a result, the FDIC incurred costs of nearly $10 million and had to revert to its legacy acquisition systems and manual reporting of some acquisition activities. We identified nearly $10 million of funds to be put to better use.[22]

Internal Control Failures and an Unaccountable Culture Resulted in an Unauthorized Contractual Commitment of $4.2 Million and a Contract Price $1.5 Million Above Market Value. In our report, FDIC Oversight of a Telecommunications Contract (March 2023), we found that the FDIC did not authorize and pay AT&T for services to upgrade bandwidth in the FDIC Field Offices in accordance with its policies and procedures and the contract. As a result, the FDIC was subject to an unauthorized contractual commitment that cost the FDIC $4.2 million and an increase in operational, monetary, legal, and reputational risks. We also found that the FDIC incurred costs above the market price for similar services in the amount of at least $1.5 million.

Lack of Contract Management Plans to Ensure Performance Risks and Contract Vulnerabilities Were Managed Appropriately. In our report, The FDIC's Adoption of Cloud Computing Services (July 2023), we found that the FDIC did not develop Contract Management Plans (CMP) for any of our sampled 17

[22] According to the Inspector General Act of 1978, a recommendation that funds be put to better use is "a recommendation by the [OIG] that funds could be used more efficiently if management of an establishment took actions to implement and complete the recommendation..." including avoidance of unnecessary expenditures noted in preaward reviews of contracts or any other savings which are specifically identified.

cloud computing-related contracts with a total value of over $546 million. We further assessed 93 active IT-related contracts and found that 91 of these 93 contracts had CMPs, but those 91 CMPs were not in place by required timeframes. Absent timely CMPs, the FDIC may not monitor performance measures, respond to missed metrics, and enforce contract penalties in a consistent manner, all of which could lead to inefficient use of resources and disruption to FDIC operations.

Ensuring the FDIC's Contracting Process Is Free from Conflicts of Interest

In our report, Conflicts of Interest in the Acquisition Process (September 2024), we found that the FDIC has processes and procedures to identify, analyze, respond to, and monitor for conflicts of interest in the acquisition process, but improvements are needed. Specifically, FDIC guidance does not require all employees involved in the acquisition planning and approval process to assess and document potential or actual conflicts of interest. We also found that the FDIC Ethics Unit has not established specialized ethics training requirements beyond the initial new employee and annual ethics training but will provide specialized training if requested by FDIC Program Offices.

Further, the FDIC's approach to confidential financial disclosure reviews could be enhanced by ensuring that financial disclosure review guidance contains clear instructions for evaluating financial disclosure forms for completeness and by training Deputy Ethics Counselors (DEC). In addition, the FDIC could enhance its approach by reevaluating the seniority, position descriptions, and number of personnel appointed as DECs, and by developing an action plan to address DEC survey responses. Absent additional internal controls throughout the acquisition lifecycle, the FDIC may not be equipped to identify, analyze, respond to, and monitor for potential or actual conflicts of interest in the acquisition process.

Contracting supports both day-to-day and crisis activities. The FDIC should have appropriate processes and internal controls to ensure that the FDIC receives goods and services it contracted for and that FDIC employees follow these processes and controls to reduce DIF operating expenses. Further, the FDIC should assess and monitor for potential or actual contracting conflicts of interest.

Ensuring IT Security and Scalability

The GAO continues to recognize cybersecurity as a high risk to Federal agencies, as it has since 1997. According to the Federal Information Security Modernization Act of 2014 Annual Report Fiscal Year 2023, 32,211 information security incidents were reported by Federal agencies in Fiscal Year 2023, which represents a 9.9-percent increase from the 29,319 incidents reported in Fiscal Year 2022.

As noted by the FDIC, "Information Technology is an essential component in virtually all FDIC business processes." The reliability and security of FDIC systems is critical, especially during a crisis. FDIC systems contain sensitive information, such as personally identifiable information on FDIC employees and contractors; bank account information for millions of depositors of failed financial institutions; confidential bank examination information, including supervisory ratings; and sensitive financial data. Further, certain FDIC systems interconnect with bank systems to receive information for examinations, quarterly Call Report data, and information from failing banks.

As described below, we have found that the FDIC can improve its IT systems security control posture and ensure that the FDIC has systems that are scalable to meet the demands of large bank failures.

Fostering IT Systems Security

In 2020, the FDIC began implementation of IT modernization activities to further develop the FDIC's cybersecurity capabilities and to shift from on-premises systems and data centers to cloud technology platforms in line with the Federal Cloud Computing Strategy. In our work, we have found that the FDIC has established several information security controls that provided either effective or adequate strategies or controls; however, this does not mean that current strategies and controls can mitigate all potential threats. As noted below, we have also identified the need for security control improvements and have made recommendations to the FDIC in the following areas:

- **Managing Systems Migration to the Cloud.** In our first report, The FDIC's Adoption of Cloud Computing Services (July 2023), we found that overall, the FDIC had an effective strategy and governance processes to manage its cloud computing services. However, the FDIC did not adhere to several cloud-related practices. As a result, any ineffective controls over cloud computing posed increased risks to the FDIC. These included security and privacy concerns due to the lack of visibility into cloud data, an inability to effectively move from one existing cloud services provider to another, not identifying and mitigating performance risks and vulnerabilities in cloud contracts, and increased potential for cyberattacks and costs from the lack of disposal strategies for legacy systems.

- **Cloud Security Controls.** In our second report, Audit of Security Controls for the FDIC's Cloud Computing Environment (September 2024), we reported that the FDIC had effective controls in four of nine cloud security control areas assessed. The FDIC had not effectively implemented security controls in five areas: identity and access management, protecting cloud secrets, patch management, flaw remediation, and audit logging. The report included 26 technical findings that pose risks to the FDIC. Malicious actors could exploit the misconfigured control settings we identified and cause harm to the FDIC's systems and data.

- **Information Security Program.** In The FDIC's Information Security Program – 2024 (September 2024), we reported that the FDIC was operating at a Maturity Level 4 (Managed and Measurable),[23] indicating an effective level of security, and established several information security program controls and practices. However, we also described security control weaknesses that reduced the effectiveness of the FDIC's information security program and practices. For example, the FDIC did not consistently maintain and document periodic audit logs of two systems that record events and activities within a computer system or network to ensure accountability, traceability, and security. Failure to perform review and analysis of these logs, specifically over privileged accounts and actions, may lead to anomalous activities that are not investigated and increase the risk that unauthorized or inappropriate activities can occur.

- **Ransomware Attack Readiness.** In our report, Review of the FDIC's Ransomware Readiness (March 2024), we determined that the FDIC had an adequate process to respond to a ransomware incident and generally followed applicable guidance and best practices within the five control areas that we assessed. We noted, however, that the FDIC did not fully adhere to Federal standards, FDIC policies, and/or industry best practices in four areas. For example, the FDIC did not effectively back up certain data and test the capability to restore two systems from back-ups and therefore could not

[23] Information regarding the assessment and determination of maturity level ratings can be found at https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act.

ensure that it would be able to successfully and fully restore these systems in the event of a ransomware incident.

Providing IT Scalability During Financial Crises

As mentioned previously, in our report, FDIC Readiness to Resolve Large Regional Banks (December 2024), we found that there were 15 identified significant technology and security gaps for the resolution of large banks due to the size and complexity of these resolutions. In addition, technology gaps identified by DRR and CISR were not sufficiently coordinated with the Chief Information Officer Organization to ensure that all resolution-related systems were adequate for a large bank resolution. The FDIC's October 2024 ERM Risk Inventory identified Resolution Technology at an elevated residual risk level with significant potential impact.

It is paramount for the FDIC to continue to ensure the availability, confidentiality, integrity, and scalability of FDIC systems and data for its day-to-day mission and during crises.

Guarding Against Harmful Scams

Scams that seek to take advantage of consumers are increasing and becoming ever more sophisticated. Scammers attempt to trick individuals into disclosing their banking information, sending money to them, or making unauthorized payments by posing as a legitimate entity such as a bank, or, as noted below, by falsely claiming affiliation with the FDIC or the FDIC OIG. Additionally, consumers may be easily duped by misrepresentations of FDIC insurance and misuse of the FDIC name and logo.

In support of the FDIC and its mission, the OIG seeks to prevent consumers from becoming victims of such fraudulent activities. Our Office of Investigations has seen a rise in various payment scams and works with law enforcement partners to pursue those who would try to deceive the public—either through payment scams or misrepresentation of FDIC deposit insurance.

A challenge for the FDIC is to be mindful of such schemes, continue to take steps to protect consumers, and take actions to address violations as appropriate.

Keeping Pace with Payment Schemes[24]

The four most common types of schemes that have been reported to the OIG have included relationship scams, investment scams, government impersonation scams, and business email compromise scams. In a relationship scam, a scammer adopts a fake online identity to gain a victim's affection and trust, and then uses the illusion of a romantic or close relationship to manipulate the victim. In an investment scam, a scammer offers low- or no-risk investments, guaranteed returns, and complex strategies to manipulate or steal from the victim. These two scams are often associated with "Pig Butchering" schemes.

A "Pig Butchering" scheme is named in reference to the practice of fattening a pig before slaughter. It is a type of confidence and investment fraud in which the victim is gradually lured into making increasing monetary contributions, generally in the form of cryptocurrency, to a seemingly sound investment

[24] See also Payment Scams: Information on Financial Industry Efforts (GAO-24-107107) (July 25, 2024).

before the scammer disappears with the contributed monies. These schemes have affected individuals and financial institutions alike. In the failed bank investigation of Heartland Tri-State Bank, for example, the bank President and Chief Executive Officer (CEO) embezzled and invested over $47 million of unsuspecting victim funds in a Pig Butchering scheme that ultimately caused the bank to fail and the DIF to incur a loss of $52.4 million. Bank customers in the small, rural Kansas community suffered greatly as well. The President and CEO was sentenced to 293 months in prison for his actions.

Recent OIG investigations have also revealed that government impersonation scams to manipulate or steal from consumers are increasingly common and often take the form of unsolicited phone calls, text messages, or e-mails that claim to be from the FDIC or FDIC OIG. Fraudsters may use the FDIC or OIG's seal or logo, and even names of actual employees, to make their demand for funds seem legitimate. (Other ramifications of misrepresentation of FDIC affiliation or insurance are outlined in the section below.)

- In cases of FDIC impersonation, scammers may contact an individual and claim that the individual has been awarded a grant or a sum of money, and the scammers may request personal information, such as bank account or credit card details, or ask for money or gift cards. These schemes often require an advance payment, which is a warning sign. According to the Federal Trade Commission's Consumer Sentinel Network Data Book, consumers reported losing over $10 billion to fraud in 2023. Impersonation scams accounted for nearly $2.7 billion of these losses, resulting from 853,935 reports.

- For FDIC OIG impersonations, scammers may contact an individual pretending to be OIG personnel, sometimes using the names of Special Agents to lend credibility to their claims. They might inform the recipient that they are under investigation and must pay a fee or fine to avoid arrest. The fee or fine is frequently requested to be paid through gift cards or other forms of payment.

Yet another type of payment scam is known as a business email compromise scam. The scammer targets a business or individual and takes over an official account, or uses email spoofing, to attempt to redirect legitimate payments to an illicit account controlled by the scammer to steal from the victim.

According to the Federal Bureau of Investigation's Internet Crime Complaint Center's (IC3) 2023 Internet Crime Report, individuals reported losing $4.57 billion to investment scams and $2.95 billion to business email compromise scams in 2023. These figures stem from 39,750 complaints and 21,489 complaints, respectively. The number of complaints of scams, and the amounts of losses, reported to the IC3 generally grew in the past 3 years.

Addressing Misuse of the FDIC Name and Logo

The FDIC obtains information on potential deposit insurance misrepresentations through two portals that are monitored by the Division of Depositor and Consumer Protection, and a third portal that is monitored by the Legal Division. The FDIC scans websites for potential fraudulent use of the FDIC logo, and the OIG Hotline also receives information regarding potential misrepresentations.

Section 18(a)(4) of the FDI Act specifically prohibits any person from harming consumers by misusing the FDIC name or logo or making misrepresentations about deposit insurance. The FDIC may investigate any

claims under this section and may issue administrative enforcement actions, including cease and desist orders, and impose civil money penalties against perpetrators.

As of December 31, 2024, the FDIC received 1,200 misrepresentation allegations through its portals, which is a 60-percent increase from the 750 allegations received in 2023. The FDIC has issued seven public cease and desist orders for these violations, and the FDIC's Legal Division, working with other stakeholders, including the OIG, has initiated the take-down of websites determined to be fraudulent and made referrals to appropriate agencies. Given the increase in misrepresentation allegations and the need to protect consumers, the FDIC should continue to ensure that it has staff and effective processes — including use of technology tools — to timely identify potential misuse and misrepresentations of the FDIC name and logo and to investigate and take action to address violations.

FDIC efforts to protect consumers from fraudulent schemes and misrepresentations can help protect taxpayer savings, provide them with trusted financial products and services, and foster public confidence in the FDIC.

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.