Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation

February 2024

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: February 22, 2024

Memorandum To: Board of Directors

/Signed/

From: Jennifer L. Fain
Inspector General

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

The Office of Inspector General (OIG) presents its annual assessment of the Top Management and Performance Challenges facing the Federal Deposit Insurance Corporation (FDIC). This document summarizes the most serious challenges facing the FDIC and briefly assesses the Agency's progress to address them.

This Challenges document is based on the OIG's experience and observations from our oversight work, reports by other oversight bodies, review of academic and relevant literature, perspectives from Government agencies and officials, and information from private-sector entities. In several instances, we discuss topic areas where the OIG had previously conducted work to evaluate, audit, and review the FDIC's progress in these Challenge areas.

We identified nine Top Challenges facing the FDIC. The Challenges identify risks to FDIC mission-critical activities and to FDIC internal programs and processes that support mission execution. These Challenges include all aspects of the Challenges that we reported last year, with important updates. Among these updates are the need for the FDIC to address increasing staff attrition--especially for examiners--and to focus on improving the FDIC's workplace environment. We also note that the failures of Signature Bank of New York and First Republic Bank demonstrated the need for the FDIC to escalate supervisory actions when risks are identified, consistent with the FDIC's forward-looking supervision initiative. Further, the FDIC should consider emerging risks in its failure estimation process and ensure that the FDIC can execute its orderly liquidation resolution authority.

The FDIC's Top Challenges include:

1. Strategic Human Capital Management at the FDIC
2. Identifying and Addressing Emerging Financial Sector Risk
3. Ensuring Readiness to Execute Resolutions and Receiverships
4. Identifying Cybersecurity Risks in the Financial Sector
5. Assessing Crypto-Asset Risk
6. Protecting Consumer Interests and Promoting Economic Inclusion
7. Fortifying IT Security at the FDIC
8. Strengthening FDIC Contract and Supply Chain Management
9. Fortifying Governance of FDIC Programs and Data

We commend the FDIC for taking steps in some areas to address certain Challenges and we note many of these actions in the attached document. This researched and deliberative analysis guides our work and we believe it is beneficial and constructive for policy makers, including the FDIC and Congressional oversight bodies. We further hope that it is informative for the American people regarding the programs and operations at the FDIC and the Challenges it faces.

Strategic Human Capital Management at the FDIC

Key Areas of Concern

The primary areas of concern for this Challenge are:

- Addressing FDIC Staff Attrition
- Managing a Wave of Prospective Retirements at the FDIC
- Sustaining a Work Environment Free from Discrimination, Harassment, and Retaliation

The FDIC relies on the talents and skills of its workforce of over 5,700 employees to accomplish its mission to maintain stability and public confidence in the Nation's financial system. The FDIC's strategic management of its human capital is important to ensure that the FDIC does not experience mission-critical skill and leadership gaps. Strategic human capital management involves a dynamic set of factors across multiple activities—workforce planning, recruitment, hiring, orientation, compensation, engagement, succession planning, and retirement programs. These activities should occur within a workplace that proactively prevents and addresses discrimination, harassment, and retaliation, and that ensures workforce diversity, equity, inclusion, and accessibility. Further, strategic human capital management involves consideration of the trade-offs of hiring permanent, temporary, or contracted staff to perform the FDIC's work.

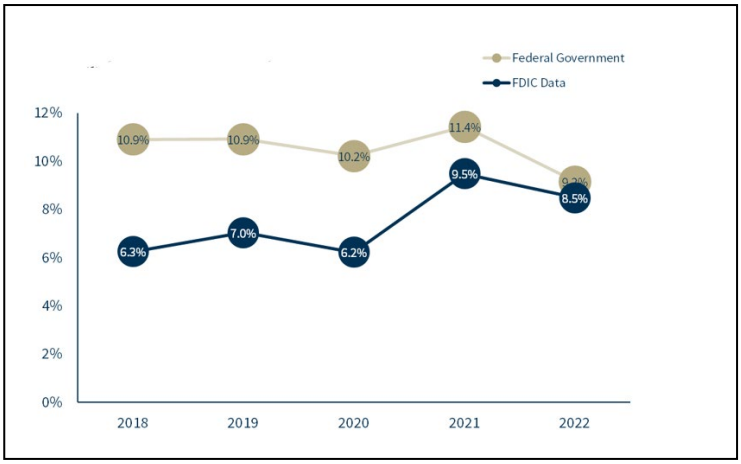
The Government Accountability Office (GAO) continues to recognize strategic human capital management as a Government-wide high-risk area, and we have included human capital risk as an FDIC Top Management and Performance Challenge since 2018. The FDIC has also included human capital management as a risk in the FDIC's Enterprise Risk Management (ERM) Risk Portfolio and in 2023 elevated the issue to the highest Enterprise Risk at the FDIC.

Addressing FDIC Staff Attrition

Attrition—through resignations and retirements—can create opportunities for employees and allow organizations to restructure, but if turnover is not strategically monitored and managed, gaps can develop in an organization's institutional knowledge and leadership.

The FDIC has faced increasing staff attrition rates, and the FDIC has been unable to close the attrition gap through hiring. As shown in Figure 1, the 2022 FDIC staff attrition rate remained higher than the pre-pandemic rates of 6.3 percent in 2018 and 7 percent in 2019. In part, the attrition increased in 2021 and 2022 because of the FDIC's Voluntary Early Retirement and Separation Incentive Program, which began in early March 2020, was suspended in mid-March 2020 as a result of the pandemic, and reintroduced in February 2021 for certain positions.

Figure 1: Workforce Attrition Rates for FDIC and Federal Government-wide 2018-2022



Source: FDIC Retention Management: Baseline Organizational Assessment

Further, the FDIC attrition rate has generally been lower than that of the Federal

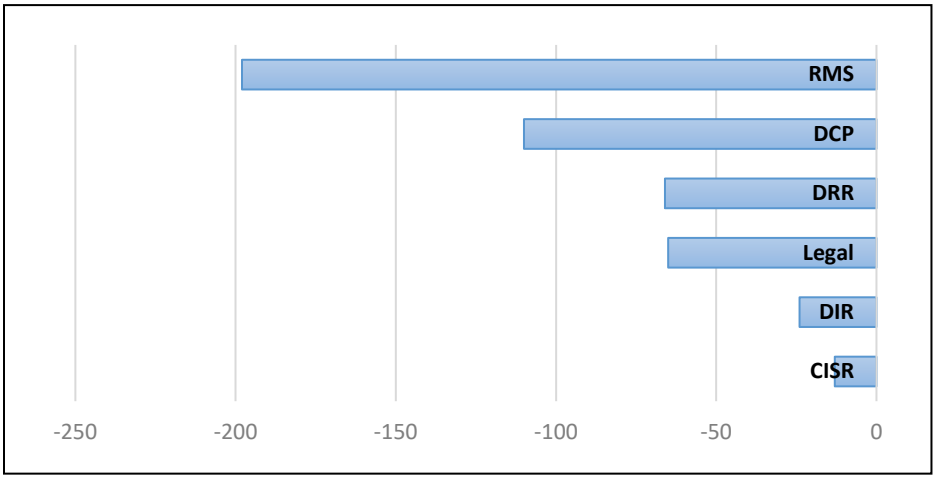
Government, but in 2022 the FDIC attrition rate was beginning to close that gap.

According to the FDIC's analysis of surveys from employees departing the FDIC, more than 41 percent of those departing were retiring, and about 25.5 percent were resigning to take positions at banks or within the private sector. Nearly 16 percent of employees transferred to other Federal agencies, and 17.5 percent did not provide a reason for departure.

FDIC staff hiring has not kept pace with FDIC attrition in all FDIC Divisions. We computed the FDIC's net gain or loss for staff hiring and attrition for the 5-year period between January 1, 2018, and January 1, 2023. As shown in Figure 2, despite hiring, important FDIC Divisions had cumulative net employee losses over that 5-year period. In other words, the FDIC lost more employees during that period than it was able to hire.

losses of over 50 staff (or about 20 percent of employees). The Legal Division, which provides legal support for all FDIC Divisions, experienced a net loss of over 50 staff (about 16 percent of employees). The Division of Insurance and Research (DIR), which analyzes emerging risks to the Deposit Insurance Fund (DIF), had net staff losses of over 20 personnel (about 14 percent of employees). The Division of Complex Institution Supervision and Resolution (CISR), responsible for the supervision and resolution of the largest banks, had net staff losses of more than 10 staff (about 5 percent of employees).

Figure 2: Cumulative Net Employee Losses (hiring less attrition) for the Period of January 1, 2018 to January 1, 2023



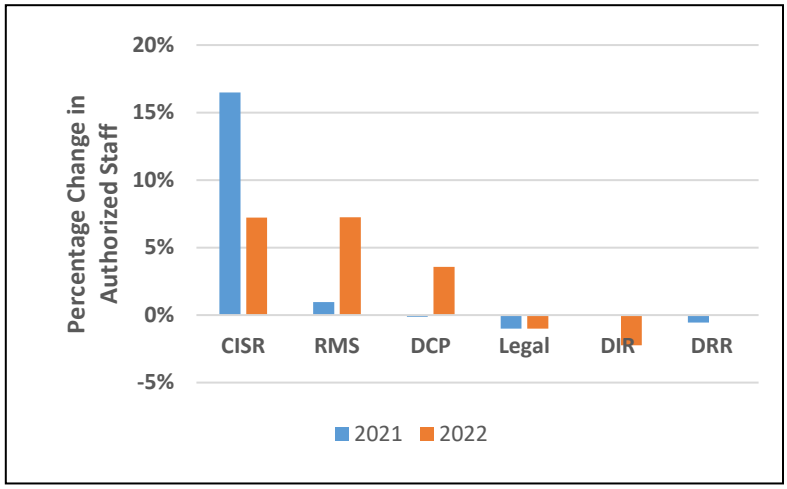
Source: OIG Analysis of FDIC Data

The FDIC's largest component, the Division of Risk Management Supervision (RMS), responsible for safety and soundness examinations and bank supervision, had a net loss of nearly 200 staff (about 9 percent of RMS employees). The FDIC's second largest component, the Division of Depositor and Consumer Protection (DCP), which conducts bank consumer compliance examinations, had a net loss of more than 100 personnel (or about 14 percent of DCP employees); the Division of Resolutions and Receiverships (DRR), responsible for marketing and resolving failed banks, paying deposit insurance, and managing bank receiverships, had net employee

Three of the six Divisions noted above also had increases in budgeted authorized staffing levels in 2021 and 2022. In effect, at the same time that the FDIC was unable to hire to replace staff losses, the FDIC determined that additional staff was needed to accomplish its mission, thereby further increasing the number of required new hires.

As shown in Figure 3, CISR had a budget authorized staffing increase of 16 percent in 2021 and 7 percent in 2022. RMS had a budget authorized staffing increase of 1 percent in 2021 and 7 percent in 2022. DCP had a budget authorized staffing increase of 4 percent in 2022. Although the Legal Division, DIR, and DRR had small percentage budget authorized staffing decreases, their respective cumulative net staff losses exceeded budget authorized staffing reductions.

Figure 3: Budget Authorized Staffing Percentage Increase/Decrease for Selected Divisions from 2021-2022



Source: OIG Analysis of FDIC Budget Data

In addition, the FDIC experienced increasing attrition for mission-critical FDIC examination staff. Examiners work in four Divisions at the FDIC: RMS, DCP, CISR, and the FDIC's Corporate University (CU). RMS examiners conduct safety and soundness examinations. According to the FDIC's Risk Management Manual of Examination Policies, bank safety and soundness examinations allow the FDIC to "identify the cause and severity of problems at individual banks and emerging risks in the financial services industry. 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." DCP examiners conduct consumer compliance examinations that the FDIC Consumer Compliance Examination Manual states "are the primary means the FDIC uses to determine whether a financial institution is meeting its responsibility to comply with the requirements and proscriptions of Federal consumer protection laws and regulations." CISR specialists, many of whom qualify as examiners, perform back-up supervision, risk monitoring and analysis, and resolution planning activities for large complex financial institutions, and examiners in CU teach examination skills to other examiner staff.

As shown in Figure 4, overall attrition among all FDIC examiners increased in 2021 and 2022 after the pandemic but began to contract in 2023. Although overall attrition rates trended lower in 2023, examiner resignations continued to increase. For 2020, examiner attrition equaled about 4 percent of all FDIC examination staff with 38 examiners resigning. In 2021, examiner attrition rose to about 6 percent with 83 examiners resigning. In 2022, about 7 percent of examiners left the FDIC with 85 examiners

Figure 4: All FDIC Examiner Resignations and Retirements 2020-2023

Source: OIG Analysis of FDIC Data

resigning. The examiner attrition rate in 2023 was 6 percent with 100 examiners resigning.

Further, turnover rates for new examiners are higher than those for new employees throughout the FDIC. The FDIC's March 2023 Baseline Organizational Assessment found that early career examiners with 2 years of training had a 15.4 percent turnover rate, but the turnover rate for non-examiner FDIC employees with 2 years of service was 4.3 percent.

Examiner departures are costly to the FDIC in terms of both funding and time. The FDIC invests approximately 4 years of training for new examiners from the time they are hired until they earn an examination commission. Such commissioning requires that employees meet benchmarks, training, and other technical requirements, including passing a Technical Examination.

Importantly, examiner departures have impacted the FDIC's mission. Both the FDIC report and our report on the failure of Signature Bank of New York found that the FDIC lacked examination resources to conduct timely, quality safety and soundness examinations.

In the FDIC Chief Risk Officer's report, FDIC's Supervision of Signature Bank, the FDIC found that it "experienced resource challenges with examination staff that affected the timeliness and quality of [Signature Bank] examinations." The report found that since 2020, 40 percent of the FDIC's New York Regional Office large bank safety and soundness examination staff positions had been either vacant or filled with temporary staff. Further, the FDIC noted challenges regarding the quality of examiner skillsets that required additional supervisory review of data analysis and reports. As a result, the report concluded that "the vacancies and adequacy of the skillsets of the Dedicated Team slowed earlier identification and reporting of [Signature Bank] weaknesses."
In our Material Loss Review of Signature Bank of New York, we found that the FDIC did not timely perform supervisory activities and was repeatedly delayed in issuing supervisory products because of staffing limitations in terms of the number of available personnel and their respective skillsets. We noted frequent turnover in the FDIC's New York Regional Office examination staff and that temporary personnel added prior to 2022 to the Signature Bank examination team often lacked requisite experience with large banks.

We recommended that the FDIC reevaluate its strategy to attract, retain, and allocate staff. Further, as discussed in greater detail in the Identifying Cybersecurity Risks in the Financial Sector section of this Report, we also found that FDIC examiner staffing impacted the ability of the FDIC to conduct timely examinations of bank third-party service providers.

Managing a Wave of Prospective Retirements at the FDIC

The FDIC also faces significant prospective retirement-eligibility risk for current staff. Retirement eligibility is the date that an employee is eligible to choose to retire, but employees may work beyond their eligibility date.

The FDIC makes annual retirement date projections beyond eligibility dates based on a combination of factors, including age and retirement eligibility. Historically, the FDIC has found that many employees have chosen to work beyond their retirement-eligibility dates.

The FDIC faces staffing risks based on its employee retirement-eligibility rates, which are higher than Government-wide averages.

As shown in Table 1, 23 percent of the FDIC workforce was eligible to retire in 2023, with that figure rising to 36 percent in 2027. According to Analytic Perspectives in the President's Fiscal Year 2023 budget, 15 percent of the Federal workforce was eligible to retire in Fiscal Year 2023 with 30 percent eligible in the next 5 years. Further, every FDIC Division except DCP had higher staff retirement-eligibility rates than the current Government-wide average retirement eligibility rate of 15 percent.

Retirement-eligibility rates are high for FDIC Executives and Managers across FDIC Regional Offices and for mission-critical examination staff.

As noted in Table 2, about 41 percent of all Executives and nearly 30 percent of all FDIC Managers were eligible to retire in 2023. These rates climb to 57 percent for FDIC Executives and nearly 47 percent for Managers by 2027. Some FDIC Regional Offices have significantly higher retirement rates for their Executives and Managers.

Table 1: FDIC Staff Retirement-Eligibility Rates by Division

Division	2023	2024	2025	2026	2027
Division of Finance (DOF)	38%	43%	46%	46%	47%
Division of Resolutions and Receiverships (DRR)	37%	42%	45%	47%	49%
Legal Division (Legal)	33%	38%	38%	48%	48%
Division of Administration (DOA)	29%	32%	36%	39%	41%
Division of Risk Management Supervision (RMS)	21%	25%	28%	32%	34%
Division of Information Technology (DIT)	18%	21%	23%	27%	31%
Division of Complex Institution Supervision and Resolution (CISR)	16%	20%	25%	27%	31%
Division of Insurance Research (DIR)	16%	21%	24%	25%	28%
Division of Depositor and Consumer Protection (DCP)	15%	19%	23%	27%	29%
Overall for FDIC	23%	27%	30%	33%	36%

Source: OIG Analysis of FDIC Data

Table 2: FDIC Executive and Manager Retirement Eligibility

	Regional Office	2023	2024	2025	2026	2027
Executives	Atlanta	100%	100%	100%	100%	100%
	Chicago	100%	100%	100%	100%	100%
	Dallas	75%	75%	100%	100%	100%
	Kansas City	100%	100%	100%	100%	100%
	New York	25%	25%	25%	50%	50%
	San Francisco	33%	67%	67%	67%	67%
	Washington	37%	42%	48%	51%	53%
	All Executives	41%	46%	52%	56%	57%
Managers	Atlanta	21%	31%	37%	40%	45%
	Chicago	22%	36%	47%	52%	56%
	Dallas	49%	53%	58%	61%	63%
	Kansas City	38%	47%	53%	58%	58%
	New York	25%	32%	39%	46%	50%
	San Francisco	24%	30%	33%	42%	48%
	Washington	28%	31%	36%	38%	40%
	All Managers	29%	35%	41%	44%	47%

Source: OIG Analysis of FDIC Data

For example, 100 percent of Atlanta, Chicago, and Kansas City Regional Office Executives and 75 percent of the Executives from the Dallas Regional Office were eligible to retire in 2023. These retirements may result in gaps in leadership positions. Leadership gaps can cause delayed decision-making, reduced program oversight, and failure to achieve Agency goals.

In addition, a significant percentage of examiners across the FDIC are eligible for retirement. As shown in Table 3, in 2023, 30 percent of supervisory examiners were eligible to retire – a figure that climbs to 53 percent in 2027. In 2023, 15 percent of non-supervisory examiners were eligible to retire, and by 2027, 29 percent of this group is eligible to retire.

Money Laundering (BSA/AML), Capital Markets, Accounting, and Consumer Protection experts. The FDIC's vulnerability to SME retirements is occurring at a time when banks are facing rising risks from the increased use of Advanced IT, partnerships with third-party service providers, involvement with crypto assets and crypto-asset sector participants, and potential fraud and money laundering risks.

Collectively, FDIC current attrition and retirement-eligibility rates have the potential to result in future organizational knowledge, skill, and leadership gaps that may impede the FDIC from achieving results.

The FDIC has recognized the significance of its human capital risk and has taken a number of steps to mitigate risks.

Table 3: Supervisory and Non-Supervisory Retirement-Eligibility Rates for All Examiners

	2023	2024	2025	2026	2027
Supervisory examiners	30%	39%	45%	50%	53%
Non-supervisory examiners	15%	19%	23%	26%	29%

Source: OIG Analysis of FDIC Data

Further, some of the examiners noted in Table 3 are considered to be subject-matter experts (SME) because they have additional training and experience in certain bank-related disciplines. As shown in Table 4, the FDIC faces significant retirement risks for SMEs. Notably, the FDIC has the highest SME retirement-eligibility rates for Advanced Information Technology (IT) and Trust Account experts followed by Intermediate IT, Bank Secrecy Act/Anti-

Table 4: Examiner Retirement-Eligibility Rates for SMEs

	2023	2024	2025	2026	2027
Advanced IT	31%	62%	62%	69%	69%
Trusts	29%	35%	39%	45%	53%
Intermediate IT	22%	24%	27%	29%	31%
BSA/AML	16%	22%	28%	33%	40%
Capital Markets	15%	21%	28%	30%	32%
Accounting	14%	24%	30%	33%	36%
Consumer Protection	7%	7%	7%	13%	20%

Source: OIG Analysis of FDIC Data

For example, in March 2023, the FDIC completed a Baseline Organizational Assessment to support the work of an FDIC-wide Retention Management Working Group. The FDIC also established a Human Capital Strategic Planning Analysis Unit within the Division of Administration to design an Agency-wide approach to address talent pipeline challenges. In September 2021, the FDIC also began its Leadership Excellence Acceleration

Program offering non-supervisory employees one year of specialized leadership training to provide the knowledge, skills, and experience to take on leadership roles. Further, FDIC Divisions have been assessing their human capital needs, including one Division that is engaging a contractor in its efforts.

Sustaining a Work Environment Free From Discrimination, Harassment, and Retaliation

Discrimination, harassment, and retaliation within an organization can have profound effects and serious consequences for the individual, fellow colleagues, and the agency as a whole. In certain instances, a harassed individual may risk losing a job or the chance for a promotion, and it may lead the employee to suffer emotional and physical consequences. It is critical for organizations to have leadership that promotes a workplace and culture that safeguards against discrimination, harassment, and retaliation.

Organizations should have policies, procedures, and training to guard against and effectively address discrimination, harassment, and retaliation. Further, organizations should have mechanisms for individuals to report incidents of discrimination, harassment, and retaliation, and processes to promptly assess reported incidents and take appropriate actions against those who engage in such misconduct.

In our July 2020 OIG evaluation, Preventing and Addressing Sexual Harassment, we assessed the FDIC's sexual harassment-related policies, procedures, training, and practices for the period January 2015 through April 2019. We found that the FDIC had not established an adequate sexual harassment prevention program and should improve its policies, procedures, and training to facilitate the reporting of sexual harassment allegations and address reported allegations in a prompt and effective manner. Specifically, we found that the FDIC had not developed a sexual harassment prevention program that fully aligned with the five core principles promoted by the Equal Employment Opportunity Commission: (1) committed and engaged leadership; (2) strong and comprehensive harassment policies; (3) trusted and accessible complaint procedures; (4) regular, interactive training tailored to the audience and the organization; and (5) consistent and demonstrated accountability.

As part of our evaluation, we conducted a voluntary survey of FDIC employees. The survey responses provided insight into employee understanding of what constitutes sexual harassment, instances of sexual harassment experienced or observed at the FDIC, impediments to reporting, and the adequacy of training. Our survey found that approximately 8 percent of FDIC respondents (191 of 2,376) said that they had experienced sexual harassment at the FDIC during the period January 2015 through April 2019.

Although 191 FDIC respondents to the OIG survey reportedly experienced sexual harassment, the FDIC only received 12 reported sexual harassment allegations, including both formal complaints and misconduct allegations from January 2015 through April 2019. This response suggests that there may have been an underreporting of sexual harassment allegations. We made 15 recommendations to the FDIC to strengthen its anti-sexual harassment program. The FDIC made changes to its anti-sexual harassment policies and procedures based on our recommendations.

On November 13, 2023, the Wall Street Journal published the first of several articles outlining a toxic work environment at the FDIC over at least a decade that alleged sexual harassment, a heavy drinking culture, improper behavior by FDIC senior leaders, and an unwillingness of employees

to file sexual harassment complaints because of the fear of retaliation. On November 21, 2023, the FDIC Board announced that the Board had established a Special Committee co-chaired by FDIC Director Jonathan McKernan and FDIC Director and Acting Comptroller of the Currency Michael Hsu to oversee a "third-party review of the agency's workplace culture." In addition, we have work ongoing to follow up on our assessment of the FDIC's sexual harassment prevention program and a Special Inquiry to report on the leadership climate at the FDIC with regard to all forms of harassment and inappropriate behavior.

Identifying and Addressing Emerging Financial Sector Risk

Key Areas of Concern

In addition to the examiner staffing challenges described in the Strategic Human Capital Management at the FDIC section of this Report, the primary areas of concern for this Challenge area are:

- Escalating Supervisory Actions to Address Identified Risks
- Assessing Emerging Risks Through Data Gathering and Analysis
- Considering Emerging Risks in the FDIC's Bank Failure Estimation Process
- Sharing Threat and Vulnerability Information with Financial Institutions

According to the FDIC's Quarterly Banking Profile, the FDIC insures over 4,600 financial institutions with total assets exceeding $23 trillion. The FDIC supervises over 2,900 of these banks with combined total assets of about $4.2 trillion. A key aspect of the FDIC's bank supervision is a forward-looking supervisory approach to identify and assess bank and banking sector risks before they impact the financial condition of a bank or the broader financial sector.

Escalating Supervisory Actions to Address Identified Risks

When FDIC examinations identify weaknesses in bank risk management, the FDIC should ensure that bank board members and senior management take timely and appropriate actions to address such risks. FDIC examinations may include recommendations requiring that bank board members address weaknesses, or in the case of severe deficiencies, the FDIC may put in place informal or formal enforcement actions to require program improvements and hold banks accountable for implementing and maintaining required changes.[1]

Prior to the financial crisis of 2008-2011, examiners identified weak risk management practices at financial institutions, but they often delayed taking supervisory action until the institution's financial performance declined. In some cases, financial decline led to bank failures and losses to the DIF.

To avoid that result, in 2011 the FDIC implemented a forward-looking supervisory initiative as part of its risk-focused supervision program. The goal of this supervisory approach was to identify and assess risk before it impacts a bank's financial condition and to ensure early risk mitigation.

Both our Material Loss Review of Signature Bank of New York and the FDIC Chief Risk Officer's report, FDIC's Supervision of Signature Bank, 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 FDIC's safety and soundness examination rating known as CAMELS[2]—changing the Management component from a 2—meaning satisfactory, to a 3—meaning needs improvement. The downgrade may have lowered the bank's composite CAMELS rating and, according to FDIC policy, supported consideration of an enforcement action against Signature Bank. We made three recommendations to the FDIC to emphasize to examiners the importance of timely escalation of supervisory concerns in line with the FDIC's forward-looking supervision initiative.

In remarks before the Committee on Financial Services, United States House of Representatives, on November 15, 2023, the FDIC Chairman noted that the FDIC was looking at options to improve supervision, such as "updating examiner guidance to be more explicit about analyses of uninsured deposit concentrations and reemphasiz[ing] to examiners the importance of forward–looking indicators of risk, such as high growth rates and breaches of internal risk limits." In our report, Material Loss Review of First Republic Bank, we recommended that the FDIC also engage with other regulators to evaluate the need for changes to rules under safety and soundness standards, including the adoption of noncapital triggers that would require early and forceful regulatory actions to address unsafe banking practices before such practices impair capital.

Assessing Emerging Risks Through Data Gathering and Analysis

The FDIC has a number of activities, beyond examinations, for the detection of emerging risks in the banking sector. The FDIC's Offsite Review Program is designed to identify emerging supervisory concerns and potential problems that may arise between onsite bank examinations so that supervisory strategies can be adjusted appropriately.[3] Further, the FDIC released its Risk Review 2023 report outlining key risks to banks. Through our work, we have found that the FDIC could do more to assess emerging risks by analyzing the data it holds and obtaining data from outside the FDIC.

Information Technology Risks. According to our report, Implementation of the FDIC's Information Technology Risk Examination (InTREx) Program, the FDIC is not fully utilizing available data and analytic tools to identify emerging IT risks at financial institutions. In 2017, the FDIC developed a tool called AlphaREx to conduct analysis of unstructured data from IT examinations. The FDIC used AlphaREx to identify financial institutions at risk from specific types of vulnerabilities, but the system has not been used to analyze FDIC IT examination data to identify emerging trends across all FDIC-supervised institutions. Such risk trend information could be used to promote risk remediation efforts, target specific IT reviews, and improve IT examination processes. Such analysis could be valuable to both policymakers and examiners in assessing cyber threats, formulating supervisory strategies, and evaluating the adequacy of InTREx procedures and examiner training. The FDIC is conducting a review to determine areas in which to use AlphaREx to identify emerging IT risks and trends at financial institutions.

Further, in our memorandum, The FDIC's Regional Service Provider Examination Program, we identified an opportunity for the FDIC to leverage available information to develop a comprehensive inventory of FDIC-supervised bank service providers. A map of bank and third-party interconnections may be useful for examiners to understand the full scope of cybersecurity risks—rather than risks solely for a single bank or third party. This information may also help FDIC policymakers to ensure that FDIC policies and examination procedures appropriately address and assess interconnected risks.

Further, in the event of a cybersecurity incident, a mapping of bank and third-party relationships may allow the FDIC to quickly identify the parties at risk and may provide relevant threat information and supervisory guidance to mitigate such risk as well as prepare for potential resolutions.

Threat Information. In our report, Sharing of Threat Information to Guide the Supervision of Financial Institutions, we found that the FDIC receives threat information relevant to the banking sector, but the FDIC had not established effective

processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions. For example, the FDIC relied solely on the judgment of certain individuals to determine the extent to which threat information should be analyzed to support FDIC business needs and the supervision of financial institutions rather than engaging stakeholders and developing procedures to guide analysis.

Also in our report, Sharing of Threat and Vulnerability Information with Financial Institutions, we found that the FDIC's threat intelligence operations may benefit from using an available natural language processing tool or alternative capabilities to analyze other FDIC unstructured data sets for the identification of threat and vulnerability information.

Government-Guaranteed Loan Information. In our report, FDIC Examinations of Government-Guaranteed Loans, we found that FDIC examiners did not have adequate data to identify, monitor, and research bank participation in Government-Guaranteed loan programs. The FDIC's DIR had obtained information from publicly-available sources for research-related purposes and studies, but that data was neither requested by nor shared with examination staff.

Absent sufficient data, the FDIC may be limited in its ability to proactively identify and monitor emerging risks associated with a bank's participation in Government-Guaranteed loan programs. Government-Guaranteed loan programs often have complex requirements and documentation standards that present compliance challenges for financial institutions. For example, a Federal agency may rescind its guaranty if a bank makes a loan to an ineligible borrower or to a borrower that lacks creditworthiness or repayment ability. The FDIC completed 6 recommendations and is in the process of implementing the remaining 13 recommendations we made to improve the FDIC's supervision of banks that participate in Government-Guaranteed loan programs.

Climate Change. As part of the Council of Inspectors General on Financial Oversight, we contributed to the Audit of the Financial Stability Oversight Council's Efforts to Address Climate-Related Financial Risk (FSOC Climate Report) that found that FSOC's Report on Climate-Related Financial Risk was consistent with Executive Order 14030, Climate-Related Financial Risk. The FSOC Climate Report identified the need for "actionable climate-related data to allow better risk measurement by regulators and in the private sector." According to the FDIC's Risk Review 2023, the FDIC is at the beginning stages of assessing climate-related financial risks. The FDIC is working with other Federal banking regulators, FSOC, and international organizations to ensure a common understanding of risks and share information.

On October 30, 2023, Federal banking regulators issued final Interagency Guidance on Principles for Climate-Related Financial Risk Management for Large Financial Institutions. The principles "provide a high-level framework for the safe and sound management of large bank exposures to climate-related financial risks."

The principles focus on governance, strategic planning, risk management, data, scenario analysis, and policies and procedures. The FDIC is also focusing on monitoring how the adverse effects of climate change could include a potentially disproportionate impact on the financially vulnerable, including low- and moderate-income and other underserved consumers and communities.

Considering Emerging Risks in the FDIC's Bank Failure Estimation Process

The FDIC estimates anticipated bank failures for its financial statements and for budgeting and planning purposes. The FDIC's internal Financial Risk Committee determines the FDIC's DIF Contingency Liability for Anticipated Failure of Insured Institutions for FDIC financial statements using a process that has been in place since at least 2015.[4] The Committee determines which institutions are included in the Contingency Liability for Anticipated Failure of Insured Institutions primarily based on bank examination CAMELS ratings, which may have up to an 18-month reporting lag. The anticipated failures figure also informs the FDIC failure estimate used for budgeting and resolution planning, which can be more forward-looking than the estimate used for the financial statements.

It is critical that the FDIC have a robust failure estimation process for its budgeting and resolution planning that monitors emerging banking risks. For example, failure estimates may need to consider the impact of the ease and speed of deposit movement through mobile apps and other technology as well as banks' unrealized losses on investment securities in assessing potential failure scenarios.

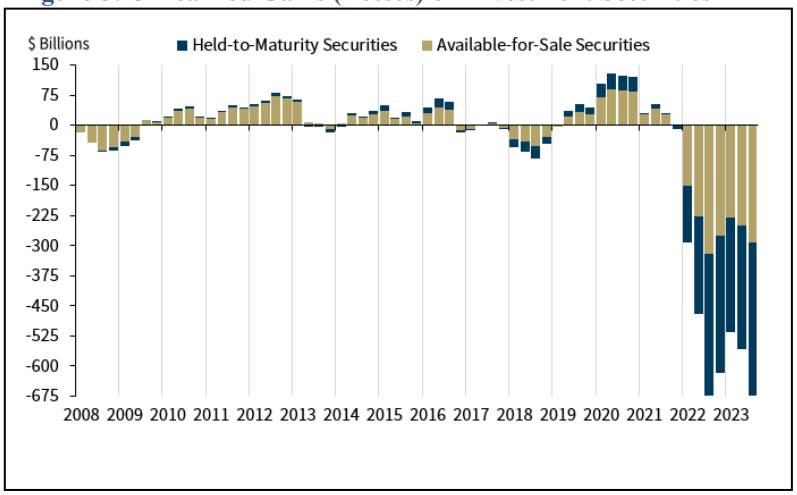
As noted in our reports, Material Loss Review of Signature Bank of New York and Material Loss Review of First Republic Bank, the speed of deposit movement and unrealized losses played a role in these bank failures. Further, as shown in Figure 5, unrealized losses on investment securities for insured banks rose again in the Third Quarter of 2023 to about $675 billion.

Sharing Threat and Vulnerability Information with Financial Institutions

A bank's Board of Directors and senior management are ultimately responsible for an institution's risk management. The FDIC, as a member of the Federal Financial Institutions Examination Council (FFIEC), has jointly stated that financial institutions should have an effective threat intelligence program, including methods for gathering, monitoring, sharing, and responding to threat and vulnerability information in order to support the institutions' safety and soundness. Without emerging threat and vulnerability information, bank board members and senior management may be unable to assess threats to their organization and take actions to reduce risks.

In our report, Sharing of Threat and Vulnerability Information with Financial Institutions, we found that the FDIC has implemented processes for sharing threat and vulnerability information with financial institutions. For example, the FDIC established formal procedures to communicate cyber threat and vulnerability information. However, the FDIC can improve the effectiveness of its processes to ensure financial institutions receive

Figure 5: Unrealized Gains (Losses) on Investment Securities



Source: FDIC Quarterly Banking Profile, Third Quarter 2023

actionable and relevant threat and vulnerability information. We determined that:

- The FDIC can improve its sharing of threat and vulnerability information with financial institutions and other financial sector entities.
- The FDIC can improve its controls over the recording of reported computer-security incidents to support threat intelligence operations and sharing activities.
- The FDIC can mature its threat information sharing program by establishing procedures for sharing non-cyber-related threat information and revising the program's existing threat sharing policies and procedures.

We made 10 recommendations to improve the FDIC's processes in order to ensure that financial institutions receive actionable and relevant threat and vulnerability information.

Ensuring Readiness to Execute Resolutions and Receiverships

Key Areas of Concern

In addition to the staffing challenges described in the Strategic Human Capital Management at the FDIC section of this Report, the primary areas of concern for this Challenge are:

- Readiness for FDI Act Resolutions
- Preparing for an Orderly Liquidation

The FDIC must stand ready to resolve failed financial institutions. The Federal Deposit Insurance Act (FDI Act) grants authority to the FDIC to execute bank resolutions and become a receiver of failed banks. The FDI Act, however, does not apply to systemically important financial companies (SIFC) such as investment banks, insurance companies, and broker-dealers. Title II of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act) was enacted and designed to address this gap and granted Orderly Liquidation Authority (OLA) to the FDIC to provide the necessary authority to liquidate failing financial companies that pose a significant risk to the financial stability of the United States in a manner that mitigates such risk and minimizes moral hazard.

Readiness for FDI Act Resolutions

The FDIC generally resolves failed banks under the FDI Act over a weekend to limit impacts to bank customers, but preparation activities for a resolution begin well before that period of time. According to the FDIC's Resolutions Handbook, the resolution process begins prior to a bank failure and includes an analysis of the bank's financial and organizational structure, receipt of failing bank data to assess a valuation, the set-up of an FDIC virtual data room to provide potential bidders information on the failing bank, the receipt of bids on the failing bank, and the FDIC's selection of a resolution strategy.

The rapid outflow of uninsured deposits during recent failures reduced the FDIC's resolution preparation lead time from days to hours. The reduced timeframe impacted the FDIC's ability to receive and validate bank data submissions from the failing banks for the establishment of an FDIC virtual data room for potential bidders.

In an August 14, 2023 speech regarding the failures of Silicon Valley Bank, Signature Bank, and First Republic Bank, the FDIC Chairman highlighted these data issues and noted shortcomings in the FDIC's 2012 rule requiring that large banks with over $50 billion in assets submit resolution plans. Specifically, the Chairman noted that the FDIC was hindered in receiving prompt and reliable information from failed banks; the FDIC did not have information on bank key personnel and retention plans, critical bank third parties, and bank payment and trading activities; and the FDIC did not have communications systems and strategies to reach internal and external stakeholders.

As noted by the FDIC Chairman, "[w]hile Silicon Valley Bank and First Republic had been required to file resolution plans which provided basic information that was useful, far more robust plans would have been helpful in dealing with the failure of these institutions. Signature Bank failed before it would have been required to file its first resolution plan in June."

Further, large bank failures also leave the FDIC with limited resolution options. For example, the FDIC can sell a failed bank or portions of its assets to another bank; however, such a transaction may increase the asset size and the systemic risk of the purchasing bank. Alternatively, the FDI Act's systemic risk exception may be

invoked—as was the case for Silicon Valley Bank and Signature Bank—when there is a serious adverse effect on economic conditions or financial stability. When invoked, the systemic risk exception allows the FDIC to resolve banks using different methods, including resolutions that may not be the least costly to the DIF. Use of the systemic risk exception may require that certain banks that had no involvement with the failed bank pay for the failed bank management's missteps.

In a series of rulemakings, the FDIC and other banking regulators are taking steps to address identified large bank resolution shortcomings. On September 18, 2023, banking regulators issued a Notice of Proposed Rulemaking that would revise regulatory capital requirements for banks with assets of $100 billion or more and for other banks with significant trading activity. Among other things, the proposed rule would change regulatory capital ratio calculations to reflect the banks' ability to absorb losses by, for example, requiring banks to include net unrealized losses on securities held as available for sale in the calculation of regulatory capital. The proposed rule has a 3-year phase-in requirement.

On September 19, 2023, banking regulators issued a second Notice of Proposed Rulemaking, requiring insured depository institutions with more than $100 billion in assets to maintain a minimum amount of long-term debt. The debt is intended to act as a "buffer" to absorb losses in the event of a bank failure, thereby providing regulators with greater flexibility to respond to the failure and reduce costs to the DIF. Currently, only the largest, global systemically important financial companies are required to hold long-term debt as part of their total loss absorbing capacity requirement.

Also, on September 19, 2023, the FDIC issued a third Notice of Proposed Rulemaking, revising a current rule requiring the submission of resolution information for insured depository institutions with $50 billion or more in total assets. The proposed rule requires that insured institutions with $100 billion or more in assets provide a full resolution plan that includes a strategy for its orderly and efficient resolution, including demonstrating the capability to provide needed information such as establishing a virtual data room with information for potential bidding parties.

Additionally, on October 11, 2023, the FDIC issued a fourth Notice of Proposed Rulemaking, providing new guidance for large banks with assets of $10 billion or more that raises the FDIC's standards for corporate governance, risk management, and controls commensurate with the size, business model, risk, and complexity of larger banks.

Further, the FDIC issued a Request for Information and Comment on Rules, Regulations, Guidance and Statements of Policy Regarding Bank Merger Transactions to receive "comments regarding the effectiveness of the existing framework in meeting the requirements of section 18(c) of the Federal Deposit Insurance Act (known as the Bank Merger Act)" including, among other things, the financial stability risks resulting from the merger of large banks. As noted by the OCC Acting Comptroller of the Currency, there is a resolvability gap for the very largest regional banks subject to the FDI Act. Should such a bank fail, the FDIC may face limited resolution options that could result in the FDIC selling the bank, or a large portion of its assets, to a systemically important financial company, thereby making the SIFC even larger and more systemic.

Preparing for an Orderly Liquidation

The FDIC has not been required to execute an OLA resolution; however, it is critical that the FDIC remain ready to do so. In our

evaluation report, The FDIC's Orderly Liquidation Authority, we determined that the FDIC has made progress in implementing elements of its OLA program, including progress in OLA resolution planning for global SIFCs based in the U.S. However, we found that in the more than 12 years since the enactment of the Dodd-Frank Act, the FDIC has not maintained a consistent focus on maturing the OLA program and has not fully established key elements to execute its OLA responsibilities. Specifically:

- **OLA Policies and Procedures.** The FDIC has made significant progress in developing high-level policies and procedures for the execution of an OLA resolution of a systemically important bank holding company. However, it has not completed operational-level policies and procedures, nor identified how it would need to adjust its policies and procedures for an OLA resolution of other types of SIFCs. In addition, the FDIC has not developed two regulations required by the Dodd-Frank Act or completed policies and procedures for ongoing OLA resolution planning activities.[5]

- **OLA Roles and Responsibilities.** The FDIC has not fully defined governance and individual practitioner-level roles and responsibilities related to the execution of an OLA resolution.

- **OLA Resources, Training, and Exercises.** The FDIC needs to obtain additional staff resources to plan for an OLA resolution, and to fully identify and document the staff and contractor resources necessary to execute an OLA resolution. In addition, the FDIC needs to enhance OLA-related training and exercises to regularly ensure that personnel have the skills needed to execute an OLA resolution.

- **Monitoring of OLA Activities.** The FDIC does not have adequate monitoring mechanisms in place to ensure it promptly implements the OLA program and consistently measures, monitors, and reports on the OLA program status and results.

- **Crisis Readiness-Related Planning.** The FDIC has not documented a readiness plan for executing OLA resolution authorities in a financial crisis scenario involving concurrent failures of multiple SIFCs.

Absent a consistent focus and fully established key elements for executing the OLA, the FDIC may not be able to readily meet the OLA requirements for every type of SIFC that the FDIC may be required to resolve. If the FDIC were unable to resolve a SIFC, the banking sector and the stability of the U.S. and global financial systems could be severely affected. The FDIC is addressing the 17 recommendations we made to improve key elements for executing the FDIC's OLA responsibilities.

Identifying Cybersecurity Risks in the Financial Sector

Key Areas of Concern

In addition to the Advanced and Intermediate IT examiner staffing challenges described in the Strategic Human Capital Management at the FDIC section of this Report, the primary areas of concern for this Challenge are:

- Examining for Bank Third-Party Service Provider Cybersecurity Risk
- Improving Bank IT Examination Processes
- Ensuring FDIC Staff Have Requisite Financial Technology Skills
- Continuing to Assess Risks Posed by Emerging Technology

In its Risk Review 2023, the FDIC recognized that the "banking industry's information technology infrastructure remains vulnerable to cyber attacks." Similarly, in its Semiannual Risk Perspective Spring 2023, the Office of the Comptroller of the Currency (OCC) found that risks to banks "continue[s] to be elevated as cyberattacks evolve and become more sophisticated and damaging to the U.S. economy." Both the FDIC and OCC have highlighted increased attacks against the banking industry through a particular variety of cyber attack known as ransomware. According to the OCC, ransomware attacks "have the potential to affect banks and market operations by rendering critical data inaccessible as well as by threatening the confidentiality of customer data through data leaks." In the 2023 Risk Management Association's survey of 100 community bank executives, 85 percent of executives stated that cybersecurity was their top risk.

Cybersecurity risks to banks include threats directed towards a bank's IT infrastructure and through attacks on banks' third-party service providers. In its Risk Review 2023, the FDIC found that "[c]yber threats to third-party providers of software, hardware, and computing services remain an important source of risk to the financial industry." For example, in August 2023, M&T Bank customer information—names, addresses, and account numbers—was compromised through a cybersecurity incident involving file transfer software used by one of the bank's third-party service providers.[6]

Examining for Bank Third-Party Service Provider Cybersecurity Risk

Banks routinely rely on third parties for numerous activities, including IT services, accounting, compliance, human resources, loan servicing, and document processing. In its Risk Review 2023, the FDIC identified multiple security risks to banks from the compromise of a third-party service provider, including "disclosure of credentials or confidential data, corruption of data, installation of malware, and application outages." In addition, multiple banks may rely on the same third-party service providers. FSOC has recognized that banks' "concentrated dependency on a limited number of service providers… [is] a potential risk to financial stability." Bank third-party risk becomes more complex when a bank's third party relies on other vendors, thereby introducing fourth-party risk to a bank.[7] In the Interagency Guidance on Third-Party Relationships: Risk Management, bank regulators noted that a bank's "use of third parties does not diminish or remove banking organizations' responsibilities to ensure that activities are performed in a safe and sound manner and in compliance with applicable laws and regulations."

The Bank Service Company Act (BSC Act) authorizes the FDIC to directly examine third-party service providers that offer services to supervised banks. The BSC Act also requires that banks notify their primary

regulator of third-party service provider relationships. Further, during bank IT examinations, the FDIC collects information regarding bank and third-party relationships.

Regulators have divided third-party service providers into two tiers based on the risks the service provider poses to the banking sector: Significant Service Providers (SSP) that serve large numbers of banks and pose a higher degree of systemic risk, and Regional Service Providers (RSP) that serve fewer banks and pose less risk. In 2012, banking regulators jointly developed guidance for risk-based examinations of service providers.[8]

In our memorandum, the FDIC's Regional Service Provider Examination Program, our objective was to assess the effectiveness of the FDIC's RSP examination program related to third-party risks to financial institutions. Overall, we found that the FDIC had not established performance goals, metrics, and indicators to measure overall program effectiveness and efficiency. As a result, we were unable to conclude on the program's effectiveness; however, we identified opportunities to improve the RSP examination program. We found that the FDIC should (1) monitor RSP examination distribution timeliness; (2) comply with examination frequency guidelines; (3) provide additional guidance on how to use RSP examinations in support of the FDIC's InTREx program (discussed in the next section below); and (4) establish a comprehensive inventory of FDIC-supervised bank service providers and the financial institutions serviced.

Significantly, our audit found that only 25 percent (18 of 71) of examinations were performed consistent with interagency guidance on examination frequency. Further, the FDIC has an opportunity to leverage available service provider information obtained through its InTREx and service provider examination programs to develop a comprehensive inventory of FDIC-supervised bank service providers.

We made one recommendation to the FDIC to 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 program effectiveness.

A full picture of the interconnected nature of IT and cybersecurity risks among banks and third parties would be helpful for examiners to understand the full scope of cybersecurity risks—rather than risks solely for a single bank or third party. This information would also help FDIC policymakers to ensure that FDIC policies and examination procedures appropriately assess and address interconnected risks. Further, in the event of a cybersecurity incident, a mapping of bank and third-party relationships may allow the FDIC to quickly identify the parties at risk and may provide relevant threat information and supervisory guidance to mitigate such risk as well as prepare for potential resolutions.

Improving Bank IT Examination Processes

FDIC 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. FDIC IT examiners follow an examination program that utilizes a risk-based approach to assess IT and cyber risks at financial institutions.

In our OIG evaluation, Implementation of the FDIC's Information Technology Risk Examination (InTREx) Program, we found weaknesses in the FDIC's InTREx program that limited FDIC examiners' ability to assess and address IT and cyber risks at financial institutions. For example, we found that examiners did not complete InTREx procedures and decision factors required to support their ratings. Without effective implementation of the InTREx

program, significant IT and cyber risks may not be identified by examiners and addressed by financial institutions. Further, an inaccurate assessment of IT risks could affect a bank's safety and soundness rating, which may require adjustments to the FDIC's supervisory strategies and examination planning for the bank and may also impact the insurance premium paid by a financial institution. The FDIC has addressed 10 of 19 recommendations we made to improve its InTREx examination processes and is working to implement the remaining 9 recommendations.

Ensuring FDIC Staff Have Requisite Financial Technology Skills

In its September 2023 report, Agencies Can Better Support Workforce Expertise and Measure the Performance of Innovation Offices, the GAO reviewed banking regulators' financial technology expertise. Financial technology includes a broad range of technology underlying bank products and services. The GAO found that the FDIC and other banking regulators "have not systematically or comprehensively collected data on their policymaking and oversight staff's technological skills related to financial technology or conducted assessments to determine the financial technology skills these staff need. The agencies also have not measured the effectiveness of their financial technology training in addressing their skill need."

Incorporating skillset assessments and measurements can help agencies ensure that staff have the skills needed to conduct effective policymaking and oversight of financial technology. The GAO made one recommendation to the FDIC to collect staff skillset data and determine the critical financial technology skills the Agency needs; develop targeted strategies to address financial technology-related skill gaps; and measure the effectiveness of its financial technology-related training in addressing skill needs.

Continuing to Assess Risks Posed by Emerging Technologies

In its 2023 Report on Cybersecurity and Resilience, the FDIC identified emerging financial sector cybersecurity threats from artificial intelligence (AI) and quantum computing. Specifically, the FDIC noted that AI may help bad actors create and refine malware that can be used to infect computer systems. AI may also be used to create malicious information, such as emails and voicemails, where the recipient—such as a bank customer—may be unable to distinguish AI-generated information from a trusted person or source—such as the bank. Further, AI may be used by malicious actors to commit synthetic fraud by creating a new person using stolen and AI-generated information.[9] It may be difficult for banks and regulators to identify such fraud.

The FDIC also noted that current data encryption methods may be vulnerable to the speed and power of quantum computing. For example, in May 2022, the Administration issued a National Security Memorandum, noting certain types of quantum computers could "defeat security protocols for most Internet-based financial transactions." The FDIC should continue to monitor risks posed by emerging technologies and ensure that necessary adjustments are made to policies, examinations, and examiner training to address such risks.

Assessing Crypto-Asset Risk

Key Areas of Concern

The primary areas of concern for this Challenge are:

- Assessing the Impact of Crypto-Asset Risks to FDIC-Supervised Banks
- Clarifying Processes for Supervisory Feedback Regarding Bank Crypto-Asset-Related Activities

FSOC describes crypto assets as private-sector digital assets that depend primarily on the use of cryptography and distributed ledger or similar technologies. In its Report on Digital Asset Financial Stability Risks and Regulation 2022, FSOC noted that "[c]rypto-asset activities could pose risks to the stability of the U.S. financial system if their interconnections with the traditional financial system or their overall scale were to grow without adherence to or being paired with appropriate regulations, including the enforcement of the existing regulatory structure." In its Annual Report 2023, FSOC noted that "some traditional financial firms were affected by shocks in the crypto-asset market." As noted by the Congressional Research Service, the failures of Silvergate, Silicon Valley, and Signature Banks "demonstrate that volatility in crypto markets may expose banks to liquidity risks that could ultimately lead to fatal losses."

The total market capitalization of crypto assets fluctuated from about $132 billion in January 2019 rising to $3 trillion in November 2021. In September 2023, crypto-asset market capitalization fell to about $1 trillion. Further, on January 10, 2024, the Securities and Exchange Commission approved 11 applications for spot bitcoin exchange traded funds, which allow investors to purchase exposure to bitcoin without directly holding bitcoin. According to FDIC data, as of September 2023, a total of 42 FDIC-supervised banks engaged in crypto-asset-related activities. Crypto-asset-related activities included, for example, deposit services, crypto-asset collateralized lending, and facilitation of customer purchase and sale of crypto assets through a third party.

Assessing the Impact of Crypto-Asset Risks to FDIC-Supervised Banks

The March 2, 2022 Executive Order on Ensuring Responsible Development of Digital Assets stated, among other things, that three of the principal policy objectives of the Administration regarding digital assets were to protect consumers, investors, and businesses; protect U.S. and global financial stability and mitigate systemic risk; and mitigate illicit finance and national security risks posed by digital asset misuse. In the January 2023 Joint Statement on Crypto-Asset Risks to Banking Organizations and the February 2023 Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities, banking regulators highlighted risks to banks from involvement with crypto assets and crypto-asset sector participants. In general, digital asset risks include:

- **Liquidity, Concentration, and Contagion Risk.** Banks face liquidity risks from crypto-asset market volatility and the resulting deposit flows associated with crypto-asset entity customers (such as a crypto exchange). For example, bank liquidity may be impacted by the size and timing of deposit inflows and outflows made by a crypto exchange on behalf of its customers. Further, deposits associated with crypto-asset reserves related to stable coins are susceptible to stable coin run risk, creating potential

deposit outflows for banks. Liquidity risk can be acute when a crypto-related entity's business represents a significant portion—or concentration—of a bank's capital, client, or business base. In addition, interconnections among crypto-asset participants—such as through lending, investing, funding, service, and operational arrangements—may cause losses for one participant to quickly flow to other participants.

- **Fraud, Illicit Finance, and Cybersecurity Risk.** Crypto-asset sector participants may not have mature and robust governance processes to manage risks. Absent oversight and governance processes, there is an increased risk of fraud, illicit activities, and cybersecurity vulnerabilities within the crypto-asset sector. Banks without effective due diligence processes may not have full insight into the activities of crypto-asset sector participants. Without effective due diligence and risk management, banks may face fines, reputational risks, and cybersecurity risks as a result of the banks' involvement with crypto-asset participant activities.

- **Consumer Protection Risks.** According to the Comprehensive Framework for Responsible Development of Digital Assets, 16 percent of American adults (approximately 53 million people) have purchased digital assets. Crypto-asset companies may make inaccurate or misleading representations and disclosures, including misrepresentations regarding Federal deposit insurance, and other practices that may be unfair, deceptive, or abusive, contributing to significant harm to retail and institutional investors, customers, and counterparties. For example, the bankruptcy filings from crypto-asset company Prime Trust detailed how the company locked itself out of its own cryptocurrency wallet and used fiat currencies from its client accounts to meet withdrawal requests. Banks engaged with crypto-asset sector participants may have exposure to these risks.

In our report, FDIC Strategies Related to Crypto-Asset Risks, we found that the FDIC has identified risks with banks' involvement with crypto-related activities; however, the FDIC has not assessed the significance and potential impact of these risks. Specifically, the FDIC has not conducted risk assessments to determine the significance of crypto-asset activity risks and the magnitude of the impact, likelihood of occurrence, and nature of the risks. Also, the FDIC has not developed mitigation strategies, such as issuing guidance to financial institutions, to ensure that risks are within defined risk tolerances. We recommended that the FDIC establish a plan with timeframes for assessing risks pertaining to crypto-related activities.

Until the FDIC assesses the risks of crypto activities and provides supervised institutions with effective guidance, the FDIC and some FDIC-supervised institutions may not take appropriate actions to address the most significant risks posed by crypto assets. Similarly, examiners may not have guidance concerning the safety and soundness and consumer protection risks of banks' involvement with crypto assets and crypto-asset participants. As a result, as banks continue to implement crypto-asset strategies, bank management and FDIC examiners may not identify and mitigate the most significant crypto-asset risks, which could lead to unsafe and unsound practices, consumer harm, or in severe instances, financial instability.

Clarifying Processes for Supervisory Feedback Regarding Bank Crypto-Asset-Related Activities

On April 7, 2022, the FDIC issued Financial Institution Letter, Notification and Supervisory Feedback Procedures for FDIC-Supervised Institutions Engaging in Crypto-Related Activities, requesting that FDIC-supervised institutions notify the FDIC if they intended to engage in, or were currently engaged in, crypto-related activities. The Letter stated that the FDIC would review the notification, request additional information as needed, and provide relevant supervisory feedback to the FDIC-supervised institution, as appropriate, in a timely manner.

In our report, FDIC Strategies Related to Crypto-Asset Risks, we found that the FDIC's process for providing supervisory feedback to FDIC-supervised institutions about their crypto-related activities is unclear. Between March 2022 and May 2023, the FDIC sent letters (pause letters) to certain FDIC-supervised institutions asking them to pause from proceeding with planned or expanded crypto activities and provide additional information. The FDIC asked the institutions to pause their activities in order to review the institutions' crypto-related activities before providing supervisory feedback.

For this pause letter process, the FDIC did not establish a timeframe for reviewing submitted information, responding to the institutions, and describing what constituted the end of the FDIC's review process. The FDIC's lack of clear procedures and timely feedback regarding crypto-asset activities causes uncertainty for supervised institutions in determining the appropriate actions to take. Absent timely feedback from the FDIC and clarity regarding the end of the FDIC's review process for paused crypto-related activities, the FDIC may be viewed as not being supportive of financial institutions engaging in crypto-related activities. We recommended that the FDIC update and clarify review timeframes and completion.

Protecting Consumer Interests and Promoting Economic Inclusion

Key Areas of Concern

In addition to the DCP examiner staffing challenges described in the Strategic Human Capital Management at the FDIC section of this Report, the primary areas of concern for this Challenge are:

- Assessing Risks in Bank Consumer Services Models
- Improving the FDIC's Ability to Increase Economic Inclusion
- Preparing to Examine for Changes to the Community Reinvestment Act
- Addressing Misuse of the FDIC Name and Misrepresentation of Deposit Insurance

According to the FDIC's 2021 National Survey of Unbanked and Underbanked Households, 96 percent of U.S. households (about 126 million in 2023) had bank accounts. In serving these households, banks must keep depositors' funds safe and treat consumers fairly, especially as banks introduce new technologies. For the 4 percent (about 5 million in 2023) of households without a bank account, the World Bank notes the importance of helping these households because access to a bank account is "a first step toward broader financial inclusion since a transaction account allows people to store money, and send and receive payments."

FDIC consumer programs and examinations seek to ensure that consumers with bank accounts are treated fairly in accordance with consumer laws and regulations. For those Americans without bank accounts, FDIC programs encourage inclusion of these individuals in the banking system to provide safe and affordable savings and credit solutions to improve household financial stability and resilience.

Assessing Risks in Bank Consumer Services Models

The Congressional Research Service has noted that banks are becoming increasingly reliant on new technology—especially AI and Machine Learning (ML). Such technology may benefit banks by allowing for "greater speed, accuracy, and confidence in loan decisions" but also introduce risks to consumers. In testimony to the U.S. House of Representatives, Committee on Financial Services, the OCC Deputy Comptroller of the Currency for Operational Risk Policy outlined key consumer risks for new technology, including:

- **Explainability.** Banks must be able to understand and explain AI decision-making processes. Absent explainability, banks may be unable to ensure compliance with laws and regulations, validate model outcomes, and ensure the absence of bias in the models' design.

- **Data management.** Banks should also understand data origins, use, and governance of analytic models to guard against unintended or illegal decision outcomes.

- **Privacy and security.** Banks must ensure the privacy and security of sensitive consumer data used by AI models.

- **Third-party risk.** Banks are also expected to have robust due diligence, effective contract management, and ongoing oversight of third parties based on the criticality of the services being provided.

On March 31, 2021, banking regulators issued a Request for Information and Comment on Financial Institutions' Use of AI, Including Machine Learning (AI RFI) to obtain information on banks' risk management processes for AI, challenges to AI adoption or use, and potential benefits to the banks for its use. Regulators are continuing to review information received from the AI RFI. Also, on October 30, 2023, the Administration issued the Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, which established standards for AI safety and security to promote innovation while protecting American consumers' privacy and civil rights.

The FDIC should ensure that its consumer protection examination procedures have processes to assess banks' use of AI and ML, and issue timely supervisory guidance to banks as needed. Further, the FDIC should ensure that its consumer compliance examination staff has sufficient skills to identify AI and ML model risk. DCP recently established a branch in the Washington Office to support DCP in assessing banks' use of emerging technologies and to monitor consumer protection risks of emerging technologies.

Improving the FDIC's Ability to Increase Economic Inclusion

In June 2019, the FDIC published its updated Economic Inclusion Strategic Plan (EISP) to guide its efforts to promote and expand economic inclusion. In our report, FDIC Efforts to Increase Consumer Participation in the Insured Banking System, we assessed whether the FDIC developed and implemented an effective EISP to increase participation in the insured banking system. We found that the FDIC's plan aligned with several strategic planning best practices. However, opportunities existed to strengthen the effectiveness of future EISPs by incorporating additional strategic planning best practices into the strategic planning process. These additional best practices included: performing a comprehensive assessment of the landscape; identifying strategies and developing outcome-based performance measures to assess progress towards desired goals; and identifying resources needed to achieve desired goals and address risks that could affect achievement of goals.

We also found that the FDIC can take steps to improve the implementation of future EISPs by aligning internal resources to achieve program objectives and measuring the outcomes of its economic inclusion efforts. Additionally, the FDIC's Enterprise Risk Management risk mitigation strategies to address economic inclusion efforts could more clearly address risks related to implementing strategic objectives, effective controls, and responsive programs to promote economic inclusion. Collectively, these actions would help management make the best use of Agency resources, ensure accountability, monitor progress, and make the EISP more effective in promoting economic inclusion. We made 14 recommendations to the FDIC to improve the development and implementation of EISPs, including the FDIC's new EISP that was under development at the time of our report.

Preparing to Examine for Changes to the Community Reinvestment Act

The FDIC must also ensure that it has required resources to devote towards changes to the Community Reinvestment Act (CRA). The purpose of the CRA is to encourage banks to help meet the credit needs of the communities in which they do business, including low- and moderate-income communities, consistent with safe and sound operations. On October 24, 2023, banking regulators issued a final rule that implements a revised regulatory framework based on a bank's asset size

and business model that uses performance tests to evaluate a bank's performance in meeting the credit needs of its entire community.

Implementation of new CRA regulations will require significant time and effort for the FDIC and the other banking agencies to revise examination policies and procedures; modify IT applications and systems; train examiners; and provide guidance and conduct bank outreach efforts. Given the staffing challenges discussed in the Strategic Human Capital Management at the FDIC section of this Report, DCP will need to ensure that it has sufficient staffing to address CRA-related changes.

Addressing Misuse of the FDIC Name and Misrepresentation of Deposit Insurance

The FDI Act prohibits any person from 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. Between July 2022 and June 2023, the FDIC issued 12 letters to non-banks requiring that the recipients stop making false and misleading statements regarding FDIC deposit insurance and take immediate action to address these misleading and false statements or to provide documentation that their claims were true and accurate.

In June 2022, the FDIC issued a final rule on its "procedures for identifying, investigating, and where necessary taking formal and informal action to address potential violations." In addition, in December 2023, the FDIC adopted a final rule to modernize its regulations governing use of the official FDIC signs and advertising statements, and to clarify the FDIC's regulations regarding false advertising, misrepresentations of deposit insurance coverage, and misuse of the FDIC's name or logo. Also, on January 19, 2024 the FDIC issued a press release stating that it demanded that five entities cease and desist from making false and misleading statements about FDIC insurance.

The FDIC obtains information on potential deposit insurance misrepresentations through various methods, including three public portals. Two portals are monitored by DCP, and the third portal is monitored by the Legal Division. The FDIC also scans websites for potential fraudulent use of the FDIC logo. We also receive information regarding potential deposit insurance misrepresentations through our OIG Hotline. The FDIC should ensure that identified potential misuse and misrepresentations are investigated and action is taken to address violations.

Fortifying IT Security at the FDIC

Key Areas of Concern

The primary areas of concern for this Challenge are:

- Strengthening the FDIC's Information Security Profile
- Improving Information Security Controls
- Managing Systems Migration to the Cloud
- Protecting the FDIC's Wireless Network
- Assessing the FDIC's Ransomware Attack Readiness

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 2022, there were 30,659 reported Federal Government cybersecurity incidents in Fiscal Year 2022, which is a 5.7 percent increase from Fiscal Year 2021.

The FDIC relies on information and systems to execute its mission. In 2023, the FDIC had five multi-year capital IT projects collectively totaling nearly $1 billion—the largest of which is the Chief Information Officer Organization's (CIOO) $862 million contract for data services. These systems contain sensitive information, such as names, Social Security Numbers, and bank account numbers for roughly 5,700 FDIC employees, about 4,300 contractors, and millions of depositors of failed financial institutions; confidential bank examination information, including supervisory ratings; and sensitive financial data. A cybersecurity incident could expose these FDIC-held data and impair FDIC mission capabilities, particularly during a crisis.

Strengthening the FDIC's Information Security Profile

The Federal Information Security Modernization Act of 2014 requires Federal agencies, including the FDIC, to conduct annual independent evaluations of their information security programs and practices. In our OIG report, The FDIC's Information Security Program – 2023 , we evaluated the effectiveness of the FDIC's information security program and practices. While the FDIC's overall information security program was operating at a Level 4 of 5, meaning managed and measurable, we found security control weaknesses that reduced the effectiveness of the FDIC's information security program and practices that could be improved:

- The FDIC needs to fully implement a software inventory automation program to manage security risks for software that is approaching or has reached its end-of-life or end-of-service.
- The FDIC's Supply Chain Risk Management program lacks maturity.
- The FDIC did not remove accounts belonging to separated personnel in a timely manner.
- The FDIC did not configure privileged accounts in accordance with the principle of "Least Privilege." We identified security risks in several instances where accounts were configured with elevated account settings that were not needed for administrators to perform their business roles, as well as other instances where users had elevated access longer than needed.

- The FDIC needs to enforce cybersecurity and privacy awareness training requirements.

The FDIC is working to implement the two recommendations we made in our report to address these control weaknesses.

Improving Information Security Controls

The FDIC should ensure that only individuals with a business need are allowed access to FDIC systems and information. The FDIC uses Active Directory to centrally manage user identification, authentication, and authorization for systems access. Active Directory infrastructure is an attractive target for attackers because the same functionality that grants legitimate users access to systems and data can be hijacked by malicious actors for nefarious purposes. Therefore, it is paramount for the FDIC to ensure that it is adequately protecting its Active Directory infrastructure.

In our OIG report, The FDIC's Security Controls Over Microsoft Windows Active Directory, we found that the FDIC had not fully established and implemented effective controls for securing and managing the Active Directory to protect the FDIC's network, systems, and data in 7 of 12 areas tested. These seven areas included password management, account configuration, access management, privileged account management, windows operating system maintenance, active directory policies and procedures, and audit logging and monitoring. The FDIC's ineffective Active Directory security controls could pose significant risks to FDIC data and systems. The FDIC has addressed 5 of the 15 recommendations we made to improve Active Directory security controls and is working to implement the remaining 10 recommendations.

In addition, in a memorandum to the FDIC during our audit, The FDIC's Information Security Program—2022, we noted potential information security and privacy issues concerning the FDIC's process to review emails flagged by certain automated tools used to detect and minimize exfiltration of information. This process presented security and privacy risks that FDIC employees and/or contractors could be inadvertently exposed to information that they would otherwise not be permitted to review, and safety risks that emails relevant to urgent law enforcement matters would not be received by the OIG in a timely manner.

In March 2023, the CIOO provided a plan to update systems and processes to ensure the confidential and timely receipt of OIG email from complainants, whistleblowers, and law enforcement partners. The FDIC has communicated that it has approved funding to further on-going efforts that the CIOO intends to take during 2024 to modernize the FDIC and OIG email infrastructure. Successful implementation, to include the resolution of technical challenges (including mail handling/data loss protection), is critical to meet the OIG's mission and maintain its independence.

Managing Systems Migration to the Cloud

The FDIC has been moving systems into a cloud environment and plans to have most of its mission essential and mission critical systems operating in the cloud by 2026. In our OIG report, The FDIC's Adoption of Cloud Computing Services, we assessed whether the FDIC has an effective strategy and governance processes to manage its cloud computing services. 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 recommended by the Office of Management and Budget (OMB),

National Institute of Standards and Technology (NIST), and FDIC guidance. As a result, controls over cloud computing posed increased risks to the FDIC, including 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 cyber attacks and costs from the lack of disposal strategies for legacy systems.

The FDIC addressed three of nine recommendations we made to address these deficiencies and continues to address the remaining six recommendations. We also have work ongoing to assess FDIC cloud security.

Protecting the FDIC's Wireless Network

The FDIC provides wireless access (WiFi) throughout its facilities. Absent effective security controls, WiFi access provides an avenue into FDIC systems that could compromise the confidentiality, availability, and integrity of FDIC data and systems.

In our OIG report, Security Controls Over the FDIC's Wireless Network, we found that the FDIC did not comply or partially complied with five practices recommended by NIST and guidance from the FDIC and other Federal agencies. As a result, the FDIC faced potential security risks based upon its then-current wireless practices and controls, including unauthorized access to the FDIC networks and insecure wireless devices broadcasting WiFi signals. The FDIC has addressed three of eight recommendations to strengthen FDIC wireless networks and is working to address the remaining five recommendations.

Assessing the FDIC's Ransomware Attack Readiness

Government agencies are being targeted by ransomware attacks involving malicious software that encrypts files, rendering them unusable until the victim pays a ransom to the perpetrator. For example, according to the GAO, in February 2023, the U.S. Marshals Service suffered a ransomware attack with perpetrators gaining access to sensitive information, including investigations and employees' personal data. In its 2023 Risk Review, the FDIC noted in particular that "[r]ansomware continues to pose a significant threat to U.S. critical infrastructure sectors, including finance and banking, as the number of attacks continues to increase."

In addition to information security safeguards, the FDIC should have effective processes to address a potential ransomware attack. A ransomware attack on the FDIC could hinder the FDIC's ability to resolve failed banks, issue deposit insurance payments to bank account holders, examine and supervise financial institutions, and manage receiverships. Disruption of any of these FDIC core functions could lead to financial system instability, including a loss of public confidence in the FDIC's ability to pay depositors.

Strengthening FDIC Contract and Supply Chain Management

Key Areas of Concern

The primary areas of concern for this Challenge are:

- Improving Contract Management
- Addressing Supply Chain Risk Management
- Ensuring Contractors Are Appropriately Vetted and Are Not Performing Inherently Governmental Functions
- Ensuring Whistleblower Rights and Protections for Contractor Personnel

Agencies should effectively manage their acquisitions process in order to ensure that contract requirements are defined clearly and all aspects of contracts are fulfilled. Agencies are also required to ensure that contractor personnel are vetted and performing appropriate tasks. Further, agencies should assess the risks of their goods and services supply chains. According to NIST "adversaries are using the supply chain as an attack vector and [as an] effective means of penetrating [United States' public and private] systems, compromising the integrity of system elements, and gaining access to critical assets." For example, in June 2023, it was reported that several Federal agencies suffered a cyber intrusion where malicious actors exploited a vulnerability in a contracted software application.[10]

Improving Contract Management

In 2023, the FDIC awarded 634 contracts for a total of $1.3 billion. GAO reviews of FDIC financial statements and our OIG reports have demonstrated a need for the FDIC to improve its contract management. In its 2020, 2021, and 2022 audits of FDIC financial statements, the GAO identified deficiencies in the FDIC's internal controls over contract documentation and payment-review processes. These deficiencies increased the risk that improper payments could occur and FDIC operating expenses and accounts payable could be misstated. Collectively, these weaknesses represented a significant deficiency[11] in the FDIC's internal controls over its financial reporting. Notably, the FDIC has been working to improve its contracting internal controls and there was no contracting significant deficiency for the 2023 financial statement audit.

In three recent OIG reports, we have found shortcomings in the FDIC's contract management process and internal controls:

- **Lack of 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), we found that the primary reason for the unsuccessful systems acquisition procurement was that the FDIC did not employ an effective change management process. The FDIC had initiated a contract to procure a new acquisition system, in part, to address weaknesses in its existing systems that were identified in our report, Contract Oversight Management. 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 contract and labor-hour costs of nearly $10 million and had to revert to its legacy acquisition systems and manual reporting of some acquisition activities. We made three recommendations to the FDIC to

improve change management. We also identified $9.9 million of funds to be put to better use.

- **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, 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 existing telecommunications contract. The FDIC did not adhere to its acquisition policies and procedures for a number of reasons. The FDIC's former CIO had not established an accountable organizational culture nor an appropriate internal control environment to ensure compliance with FDIC acquisition policies and procedures. The FDIC CIOO and DOA did not implement proper internal controls for the AT&T contract. Additionally, the FDIC did not include risks related to the FDIC CIOO's reliance on contractor services and the need to maintain an effective internal control environment for its contract oversight management activities in the FDIC Enterprise Risk Management's Risk Inventory. Further, certain FDIC CIOO personnel did not fulfill their roles and responsibilities. As a result, the FDIC was subject to an unauthorized contractual commitment that cost the FDIC $4.2 million and a prolonged increase in operational, monetary, legal, and reputational risks. Further, we found that the FDIC incurred costs above the market price for similar services in the amount of at least $1.5 million. The FDIC has addressed 10 of 14 recommendations we made to improve organizational culture and establish internal controls.

- **Lack of Contract Management Plans to Ensure Inherent Performance Risks and Contract Vulnerabilities Were Managed Appropriately.** In our report, The FDIC's Adoption of Cloud Computing Services, we found that the FDIC did not develop Contract Management Plans (CMP) for any of our sampled 17 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. CMPs are developed to document a common understanding of contractor and FDIC obligations and provide a strategy for managing key contract vulnerabilities or performance areas inherent in the contract, and any unique contract terms and conditions. Absent 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. The FDIC addressed three of nine recommendations we made to address these deficiencies and continues to work to address the remaining six recommendations.

The FDIC must also ensure that employees involved in contracting do not have conflicts of interest. According to the FDIC's Ethics Program Advisory, Conflicts of Interest, FDIC employees are trusted to make decisions and take actions to serve the public's interest and should not act to enrich their own personal interests. The Advisory also notes that criminal penalties—felony conviction, fines, or jail time—could result from conflicts of interest.

Addressing Supply Chain Risk Management

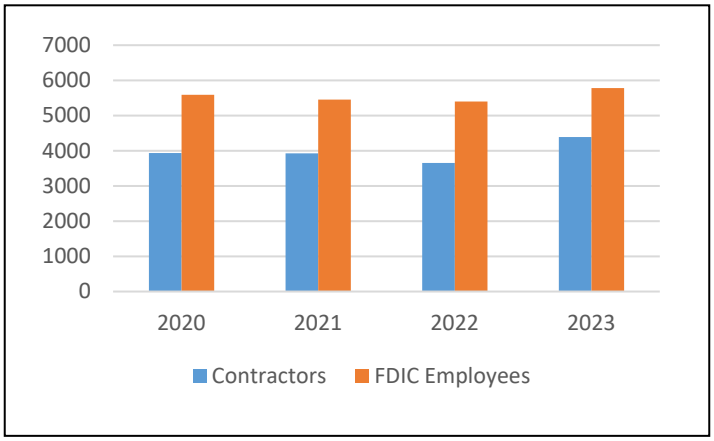
In our report, The FDIC's Implementation of Supply Chain Risk Management, we found that the FDIC has not implemented several objectives outlined in its Supply Chain Risk Management Implementation Project Charter and is not conducting supply chain risk assessments in accordance with best practices. In addition, we found that the FDIC has not integrated Agency-wide supply chain risks into its Enterprise Risk Management processes. The FDIC has addressed four of nine recommendations we made to improve the FDIC's supply chain risk management process and is working to address the remaining five recommendations.

As part of our later OIG report, The Federal Deposit Insurance Corporation's Information Security Program -2023, we found that the FDIC's supply chain risk management program lacked maturity because five of nine recommendations from our Supply Chain Risk Management report remained outstanding. Specifically, the FDIC had not completed development of policies and procedures to address supply chain risk and had not conducted supply chain risk assessments prior to entering into contracts with new suppliers or when substantive changes were made to contracts, such as renewals, extensions, or exercising option periods. Further, the FDIC had not established required metrics and indicators to monitor and evaluate supply chain risk and implement supply chain controls recommended by NIST.

Ensuring Contractors Are Appropriately Vetted and Are Not Performing Inherently Governmental Functions

The FDIC budget for 2023 included $458 million for outside services—which was the second highest budget category behind employee salary and benefit costs. As shown in Figure 6, the FDIC has consistently had about 4,000 contractors supporting the FDIC permanent staff of about 5,700. The FDIC increased contractor staffing in 2023 because of bank failure activity.

Figure 6: FDIC Employees and Contractors 2020 to 2023



Source: OIG Analysis of FDIC Data

Contractors must meet FDIC and Government-wide vetting standards before they may begin work at the FDIC. As part of our work reviewing the FDIC's IT security controls, we found that the FDIC did not have adequate controls to ensure that certain contractors and employees who required privileged access to FDIC information systems and data had background investigations commensurate with appropriate determinations of risk.

In our memorandum regarding these inadequate controls, Background Investigations for Privileged Account Holders, we alerted the FDIC that one contractor who met FDIC standards in February 2021 was granted access to a privileged account in April 2021. However, the Federal background investigation was not adjudicated until November 2021, and the adjudication was unfavorable at that time. Based on the adjudication, the FDIC ceased the privileged access and terminated the contractor, consistent with FDIC policies and procedures. The

contractor had access to privileged accounts for approximately 7 months while the background investigation was being adjudicated.

Also, certain functions cannot be performed by contractors. In OMB Policy letter 11-01, Performance of Inherently Governmental and Critical Functions, OMB defined these functions as inherently governmental functions. OMB also required that most agencies identify critical functions and ensure sufficient staffing and control over these functions.[12] OMB defined a Critical Function as "a function that is necessary to the agency being able to effectively perform and maintain control of its mission and operations. Typically, critical functions are recurring and long-term in duration."

In our OIG evaluation, Critical Functions in FDIC Contracts, we assessed whether an FDIC contractor performed Critical Functions and, if so, whether the FDIC retained sufficient management oversight of the contractor to maintain control of its mission and operations in accordance with best practices. We found that the FDIC did not have policies and procedures for identifying Critical Functions in its contracts. Therefore, while we determined that the contractor performed Critical Functions at the FDIC, the FDIC did not identify these services as Critical Functions during its procurement planning phase. As a result, the FDIC also did not implement heightened contract monitoring. The FDIC has addressed 11 of our 13 recommendations to strengthen the FDIC's identification and monitoring of contracts involving Critical Functions, and the FDIC is working to address the remaining 2 recommendations.

Ensuring Whistleblower Rights and Protections for Contractor Personnel

In our OIG report, Whistleblower Rights and Protections for FDIC Contractors, we found that the FDIC had not aligned its procedures and processes with laws, regulations, and policies designed to ensure notice to contractor and subcontractor employees about their whistleblower rights and protections. The FDIC also did not always comply with the requirements to notify contractors of their whistleblower rights and protections. The FDIC's Legal Division did not adopt any whistleblower rights notification provisions for contractors or include any whistleblower clauses in its contracts. The FDIC also did not verify that contractors and subcontractors notified employees of their whistleblower rights and protections.

The FDIC has implemented eight of our nine recommendations, including the Legal Division's adoption of whistleblower rights notifications and inclusion of whistleblower clauses. The FDIC is working to resolve the remaining recommendation to develop and implement procedures to ensure that contractors carry out their obligations to verify that all contractor and subcontractor personnel are notified of their whistleblower rights and that whistleblower clauses are included in subcontracts.

Fortifying Governance of FDIC Programs and Data

Key Areas of Concern

The primary areas of concern for this Challenge are:

- Strengthening Performance Goal Development and Monitoring
- Improving Internal Controls by Addressing Outstanding Recommendations
- Ensuring Data Quality to Assess Program Performance

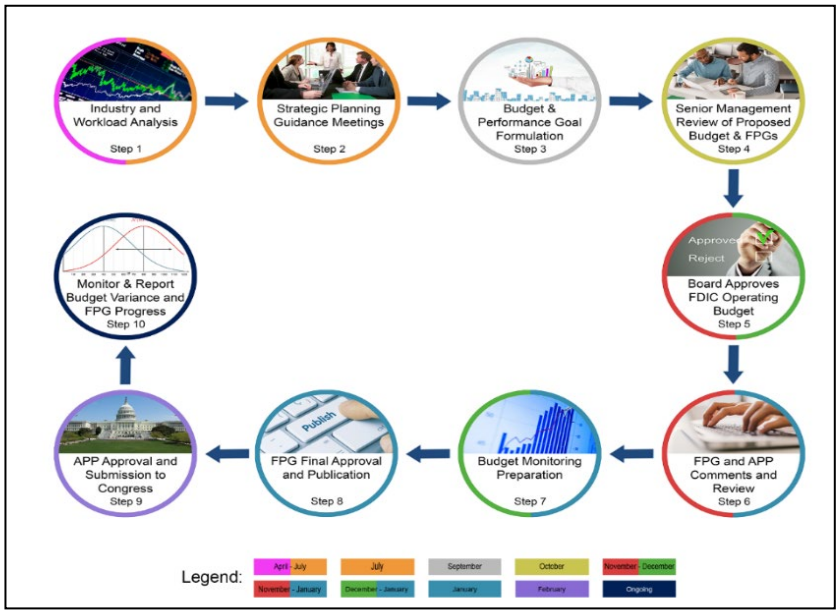
Effective governance is critical to ensure that the FDIC assesses and addresses risks—especially those identified in this Report. Governance refers to a management framework that incorporates operational, financial, risk management, and reporting processes, so that FDIC Board Members and senior officials can effectively plan, govern, and meet strategic objectives. This includes ensuring alignment of goals, budget, and risks to achieve the FDIC's mission. A governance framework should ensure strategic guidance, effective monitoring of management, and accountability to stakeholders.

Strengthening Performance Goal Development and Monitoring

The FDIC develops and monitors its performance goals as part of the FDIC's annual planning and budget process. The FDIC annual planning and budget process is key to providing resources—funding, staffing, goods, and services—for the FDIC to address and measure progress towards tackling identified challenges.

As shown in Figure 7, the FDIC's annual planning and budget process is continual and includes ten steps: (1) industry and workload analysis, (2) strategic planning, (3) budget and performance goal development, (4) senior management review of the budget and performance goals, (5) Board approval of the budget, (6) internal FDIC performance goal and annual performance goal review, (7) budget monitoring, (8) approval of internal FDIC performance goals, (9) approval of external annual performance goals and submission of these goals to Congress, and (10) monitoring and reporting budget variance and progress in achieving FDIC internal performance goals.

Figure 7: FDIC Annual Planning and Budget Process



Source: FDIC DOF Website

The FDIC's annual planning and budget process also considers risks identified through the FDIC's ERM process. According to the GAO, ERM "is a forward-looking approach that allows agencies to assess threats and opportunities that could affect achievement of its goals." OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, notes

that ERM should be part of an agency's strategic planning, performance management, and performance reporting.

In a number of our reports, we have found limitations in the FDIC's development and monitoring of FDIC performance goals and a misalignment between performance goals and FDIC strategic plans that impeded the FDIC from assessing and measuring progress towards goal achievement. For example:

- **Bank IT Examinations:** In our report, Implementation of the FDIC's Information Technology Examination (InTREx) Program, we found that the FDIC's performance goal focusing on improving its supervision program did not focus on IT supervision activities and did not address the performance of IT examinations or the effectiveness of the InTREx Program. Also, in the RMS Division Strategic Plan 2018-2022, RMS established the following performance goal: "RMS supervision is effective, forward-looking, and provides value-added risk management expertise to banks." However, this goal does not directly address the FDIC's InTREx program. Without establishing IT examination performance goals, objectives, and metrics, the FDIC is unable to measure the effectiveness of the InTREx program. Further, the FDIC is unable to determine whether its IT examination activities under the InTREx program are achieving their desired outcomes or results.

- **Regional Service Provider Examinations:** In our memorandum, The FDIC's Regional Service Provider Examination Program, we found that the FDIC has not established performance goals or metrics to measure the effectiveness of the RSP examination program. Establishing performance goals and metrics for the RSP examination program would allow the FDIC to define program expectations and measure overall program efficiency and effectiveness, which would identify areas for improvement.

- **Orderly Liquidation Readiness:** In our report, The FDIC's Orderly Liquidation Authority, we found limitations in the FDIC's monitoring and reporting of Division and Agency-level goals and objectives related to OLA. Specifically, we found that monitoring and reporting activities did not ensure OLA resolution planning activities had consistently and promptly progressed since the enactment of the Dodd-Frank Act nor did they provide a clear picture of the overall status of the OLA program. The FDIC had not developed long-term metrics and a clear definition of success that would facilitate consistent measuring, monitoring, and reporting on the overall status of the OLA program over time. Such metrics could address key readiness items such as the status of readiness plans, policies and procedures, training activities, processes subjected to exercises, and outstanding significant action items from exercises.

  Further, we found that in 2015, the FDIC had established an annual performance goal to "[e]nsure the FDIC's operational readiness to resolve a large, complex financial institution using the orderly liquidation authority in Title II of the DFA." A key target for reaching this goal, identified in the FDIC Annual Report 2015, was to "Update and refine firm-specific resolutions [sic] plans and strategies and develop operational procedures for the administration of a Title II

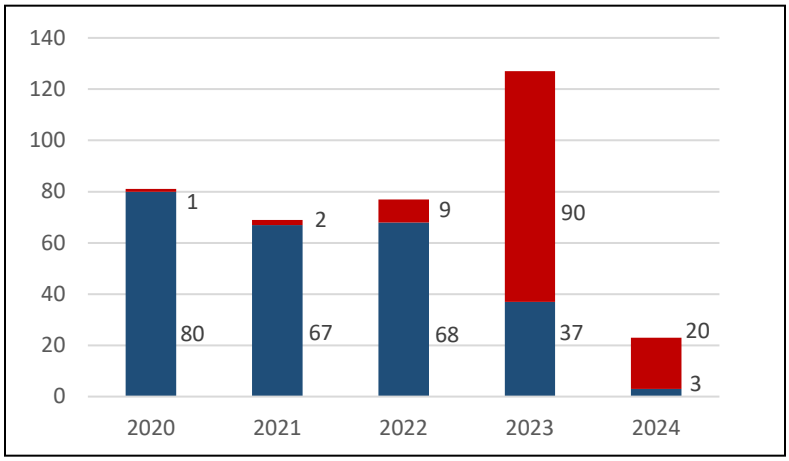
receivership." The FDIC reported this milestone as achieved, in part because the FDIC had developed its Systemic Resolution Framework. However, the 2015 annual report did not clearly reflect the overall status of the OLA program, which continues to lack the process-level procedures needed for the Systemic Resolution Framework and the resolution strategies needed for an OLA resolution of a systemically important non-bank financial company or Financial Market Utility.

- **Increasing Consumer Participation in Banking:** In our report, FDIC Efforts to Increase Consumer Participation in the Banking System, we found that the FDIC could strengthen connections between FDIC Annual Performance Goals and DCP's Economic Inclusion Strategic Plan (EISP) by ensuring that the expressed intent of annual goals related to DCP's economic inclusion efforts matched the goals and objectives articulated in the EISP. We also found that the FDIC could improve the implementation of future EISPs by aligning internal resources to achieve program objectives and measuring the outcomes of its economic inclusion efforts. Collectively, these actions would help management make the best use of Agency resources, ensure accountability, monitor progress, and make its strategic plan more effective in promoting economic inclusion.

Improving Internal Controls by Addressing Outstanding Recommendations

As shown in Figure 8, as of January 31, 2024 the FDIC had 122 OIG report recommendations that were unimplemented – meaning the OIG had not received and reviewed information from the Agency to indicate that a recommendation should be closed. A total of 90 percent (110 of 122) of unimplemented recommendations were for reports issued during Fiscal Year 2023 and 2024, while 10 percent (12 of 122) related to reports issued between Fiscal Year 2020 and 2022.

Figure 8: Unimplemented Recommendations by Fiscal Year



Source: FDIC OIG website

The longest outstanding recommendation is for our report, Contract Oversight Management. In 2019, we recommended that the FDIC provide enhanced contract portfolio reports to the FDIC Board of Directors, executives, and senior managers. Further, four recommendations remain outstanding from our 2021 report, Critical Functions in FDIC Contracts. As noted in the Strengthening FDIC Contract and Supply Chain Management section of this Report, contract management remains a significant challenge at the FDIC and has been identified by the FDIC as high risk in the FDIC's Risk Inventory. The FDIC Board and senior officials should ensure that program weaknesses are promptly resolved. If recommendations are not addressed expeditiously, the FDIC faces an increased likelihood that the underlying vulnerabilities or deficiencies will continue or recur until remediated by the FDIC.

Ensuring Data Quality to Assess Program Performance

Data is one of the most valuable FDIC assets. Analytical insights based on reliable data can support evidence-based decision making and help the FDIC build a performance-based culture. Reliable data requires effective governance of the data lifecycle from the point that data is entered into a system through the retirement of data records. Inadequate data governance can lead to higher costs, incorrect decisions, and reputational risks to the FDIC. Further, data quality is an important control in implementing effective use of artificial intelligence. Prior reports[13] and three recent reports highlight data reliability issues:

- **Bank-reported Computer Security Incidents:** In our report, Sharing of Threat and Vulnerability Information with Financial Institutions, we determined that the FDIC's controls were not effective to ensure that it maintained complete and accurate data in the Virtual Supervisory Information on the Net system on all computer-security incidents reported by banks and service providers. Inaccurate and incomplete incident information may limit the FDIC's ability to conduct critical research and trend analyses on threats and vulnerabilities and impede its ability to share accurate, complete, and relevant information internally with its examination staff and externally with financial institutions.

- **Human Capital Costs Related to Economic Inclusion Efforts:** In our report, FDIC Efforts to Increase Consumer Participation in the Insured Banking System, we identified data reliability issues with reports created out of the Community Affairs Reporting and Events System used to plan, monitor, and track outcomes of economic-inclusion related events and activities. As a result of data reliability issues, the FDIC cannot ensure it is allocating resources to its economic inclusion-related activities efficiently, effectively, or with accountability to achieve the Agency's goals.

- **RSP Bank Customer List:** In our memorandum, The FDIC's Regional Service Provider Examination Program, we noted that the RSP Uniform Customer List—the list showing the banks with whom the RSP has contractual obligations for services—was found by the FDIC to be unreliable. As a result, the FDIC and other Federal banking regulators were unable to distribute their reports of examination for RSPs to the banks that received the RSP's services.

The FDIC should have an Agency-wide approach to data quality. Each FDIC Division and Office should ensure that the data they gather and enter into systems is adequate, appropriately controlled, and used effectively to improve operations. FDIC Divisions and Offices should also partner with the FDIC's Division of Information Technology to use technology to assess and test for data quality issues. The FDIC's cloud migration effort includes data quality reviews to identify unreliable data prior to cloud migration, and Divisions and Offices should ensure that they have resources to address data issues as they are identified.

[1] Informal actions are voluntary commitments made by a bank's Board of Directors that are not legally enforceable and are not publicly disclosed or published. Examples of informal enforcement actions are a Bank Board Resolution or a Memorandum of Understanding. Formal actions are legally enforceable and published on the FDIC website. Examples of formal enforcement actions are Consent Orders or Cease and Desist Orders.

[2] According to the FDIC RMS Manual, RMS examination staff assess and rate six financial and operational components - **C**apital adequacy, **A**sset quality, **M**anagement capabilities, **E**arnings sufficiency, **L**iquidity position, and **S**ensitivity to market risk - commonly referred to as CAMELS ratings. Examiners assign the component and composite ratings based on a numerical scale from 1 to 5, with 1 indicating the strongest performance and risk management practices. A 5 rating indicates the highest degree of supervisory concern.

[3] *See* OIG report, Offsite Reviews of 1- and 2-Rated Institutions (December 2019), for a description of the Offsite Review Program.

[4] The process is based on generally accepted accounting principles.

[5] The FDIC has not yet completed the following OLA requirements to prescribe correlating rules or regulations for: (1) 12 U.S.C. § 5390(o)(6) that requires the FDIC, in consultation with the Secretary, to prescribe regulations to implement assessments of U.S. financial companies, if such assessments are needed, to pay in full obligations issued by the FDIC to the Treasury, and (2) 12 U.S.C. § 5393(d) that requires the FDIC and the FRB, in consultation with FSOC, to jointly prescribe rules or regulations to administer and carry out a ban on activities by senior executives and directors of failed SIFCs if they have violated a law, regulation, or certain agency orders; or participated in "any unsafe or unsound practice" in connection with a financial company; or breached their fiduciary duties. Specifically, the DFA authorizes the FDIC or FRB, as applicable, to "prohibit any further participation by such person, in any manner, in the conduct of the affairs of any financial company for a period of time determined by the appropriate agency to be commensurate with such violation, practice, or breach, provided such period shall be not less than 2 years."

[6] NBC, Some M&T Bank Customer Information Hacked in Massive Data Breach (August 30, 2023).

[7] American Banker, This is the Sleeping Giant, Banks Zero in on Fourth-Party Risk (August 4, 2023).

[8] *See* FFIEC, Financial Regulators Release Guidance for the Supervision of Technology Service Providers (October 31, 2012) and current guidance Supervision of Technology Service Providers.

[9] American Banker, AI Is About To Make Synthetic Fraud A Much Bigger Problem (July 4, 2023).

[10] CNN, Exclusive: US Government Agencies Hit in Global Cyberattack (June 15, 2023).

[11] A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis.

[12] The FDIC found that Policy Letter 11-01 was not binding on the FDIC, but the FDIC has viewed the policy as instructive.

[13] *See* our reports: The FDIC's Personnel Security and Suitability Program, where we found that contractor position risk levels recorded in FDIC systems were unreliable. As a result, the FDIC could not determine whether these contractors received background investigations commensurate with their positions. Termination of Bank Secrecy Act/Anti-Money Laundering Consent Orders, where we found that the FDIC did not consistently track Consent Order termination data in its system of record. As a result, the FDIC provided nine incorrect reports to the FDIC Board of Directors concerning enforcement actions and did not report three BSA/AML Consent Order terminations in a quarterly report to FinCEN. Reliability of Data in the FDIC Virtual Supervisory Information on the Net System, where we found that two of the four key data elements we tested in the FDIC's ViSION system were not reliable. Errors in these data elements increase the risk of inaccurate reporting of examination performance metrics to FDIC management.

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.