Information Resource Management Strategic Plan

August 2025

Federal Deposit Insurance Corporation
Chief Information Officer Organization

Contents

1. Introduction

This Information Resource Management (IRM) Strategic Plan outlines how the Federal Deposit Insurance Corporation (FDIC) will manage its information technology (IT) resources to fulfill its statutory mission of insuring deposits; supervising financial institutions for safety, soundness, and consumer protection; making large and complex financial institutions resolvable; and managing receiverships. The plan describes how the FDIC integrates its IRM planning and investment decision-making with agency budget formulation and execution, human resources management, and business programs and operations. In developing this IRM Strategic Plan, the FDIC considered relevant provisions of Federal statutes and government-wide directives and guidance, including the Federal Information Security Modernization Act of 2014 (FISMA), the Paperwork Reduction Act, the Office of Management and Budget's (OMB) Circular No. A-130—*Managing Information as a Strategic Resource*, and the Federal Cloud Smart Strategy. This IRM Strategic Plan also aligns with the goals and objectives in the FDIC 2022-2026 Strategic Plan and areas of focus identified by the FDIC Acting Chairman.

Consistent with the Government Performance and Results Act (GPRA)[1] and OMB policy,[2] the FDIC is working to revise its agency Strategic Plan to capture the priorities of the current Administration. The Chief Information Officer (CIO) Organization (CIOO) is actively participating in this effort. Once the FDIC completes its work to revise the agency Strategic Plan, the CIOO will update and finalize the Implementation Actions in the four Strategic Focus Areas described later in this IRM Strategic Plan. Thereafter, the CIOO will update this IRM Strategic Plan annually to reflect progress in addressing the Implementation Actions, as well as changes in agency priorities and new compliance or regulatory requirements.

As a steward of public trust and a key pillar of the U.S. financial system, the FDIC is committed to the principles of transparency, accountability, and public access to information. In this regard, this IRM Strategic Plan includes the FDIC's Open Data Plan as mandated by the Open, Public, Electronic & Necessary Government Data Act (OPEN Government Data Act). The Open Data Plan, which aligns to the Federal Data Strategy, provides a framework to manage and expand the publication of FDIC's data assets, ensure data quality, engage with stakeholders, and contribute to the government-wide Federal Data Catalog. As described in the Open Data Plan, the FDIC seeks to maximize the use and reuse of its data to inform research, improve policy, and empower the public.

IT Governance and Management

1.1. Authorities of the Chief Information Officer

The FDIC Board of Directors (FDIC Board) has delegated overall responsibility for managing the

[1] As modified by the GPRA Modernization Act of 2010 and certain provisions of Title I, Federal Evidence-Building Activities of the Foundations for Evidence-Based Policymaking Act of 2018.
[2] OMB Circulars No. A-11, *Preparation, Submission and Execution of the Budget*, and A-130, *Managing Information as a Strategic Resource*.

Corporation's IT program and operations to the CIO. The CIO reports directly to the FDIC Chairman and has broad strategic responsibility for IT governance, investments, program management, information security, and IT modernization activities that advance the FDIC's technology vision. The CIO's responsibilities include ensuring compliance with relevant laws and government-wide mandates, and managing the day-to-day operations and maintenance of a complex IT infrastructure and more than 200 information systems that support core business functions and related support activities. The CIO also serves as the FDIC's Chief Privacy Officer and Senior Agency Official for Privacy. In these roles, the CIO has responsibility for establishing and implementing a wide range of privacy and data protection policies and procedures pursuant to legislative and policy requirements.

To safeguard the confidentiality, integrity, and availability of its information systems and data, the CIOO maintains an agency-wide information security program. The FDIC's Chief Information Security Officer (CISO), who reports to the CIO and the FDIC Chairman, is responsible for managing the information security program.

In response to Federal statutes and government-wide guidance directing agencies to modernize their data management practices, the FDIC established a Chief Data Officer (CDO) position within the CIOO in 2019. The CDO reports to the CIO and has agency-wide responsibility for promoting effective understanding, management, governance, and strategic use of data to drive business value in support of the FDIC's mission. This includes developing enterprise data governance, policies, processes, and ensuring relevant FDIC data are shared with the public in a timely manner. The CDO also leads strategic data initiatives, such as the development of an enterprise data inventory, the implementation of a Cloud Data Management and Analytics initiative, and the adoption of artificial intelligence (AI) capabilities.

1.2. IT Governance

The FDIC has established an IT governance structure and supporting processes to ensure compliance with relevant laws and government-wide policy and guidance, as well as to ensure the agency's IT functions and operations effectively support business strategies and operations. Effective IT governance is critical for ensuring the delivery of high-quality IT products and services that support the FDIC's priorities, satisfy customer expectations, and meet cost, schedule, and performance expectations.

The FDIC has modeled its IT governance and processes on various statutes, such as the Paperwork Reduction Act and FISMA, OMB policy and guidance, and National Institute of Standards and Technology (NIST) security standards and guidelines. Of note, OMB Circular A-130—*Managing Information as a Strategic Resource* requires Federal agencies, including the FDIC, to establish and implement fundamental components of IT governance that include (among other things) an:

- **IRM Strategic Plan** that describes the agency's technology and information resources goals. The IRM Strategic Plan supports the goals and objectives in the Corporation's Strategic Plan and demonstrates how the technology and information resources goals relate to agency mission and priorities.

- **Enterprise Architecture** (EA) that describes the FDIC's baseline IT architecture, target architecture, and plans for transitioning to the target architecture. The EA links business goals and priorities with technology to ensure IT solutions meet agency business requirements. The EA is critical to the successful implementation of this IRM Strategic Plan because the EA defines the roadmap and sequencing plan for executing the Corporation's IT initiatives.

In addition to the agency Strategic Plan, IRM Strategic Plan, and EA, the FDIC establishes Annual Performance Goals and FDIC Performance Goals to measure progress in addressing IT priorities. The FDIC has also established various governance bodies, including the Capital Investment Review Committee (CIRC), CIO Council, the Enterprise Data Council (EDC), and the Security and Enterprise Architecture Technical Advisory Board (SEATAB) to oversee and monitor the implementation of IT strategies, policies, projects, and spending. A brief description of these governance bodies follows.

- **CIRC.** The FDIC established the CIRC in 2003 to review, approve, and monitor major IT and non-IT investment projects with estimated capital outlays of $10 million or more, as well as certain other projects that cost less but are considered mission-critical and/or high risk to the FDIC. The CIRC meets quarterly to provide ongoing oversight of these projects to ensure that they are properly managed, that risks are proactively addressed, that cost and performance targets are met, and that business value and alignment with the EA is achieved. The CIO and Chief Financial Officer co-chair the CIRC.
- **CIO Council.** The FDIC established the CIO Council in 2005 to advise the CIO on the adoption and use of IT at the FDIC. The Council's members consist of senior executives from the FDIC's Divisions and Offices who have delegated authority to agree to and authorize IT decisions on behalf of their organizations. These members advise the CIO on business priorities and the effect of IT and information security decisions on agency business operations. The CIO chairs the CIO Council, which meets monthly.
- **EDC.** The FDIC established the EDC in 2020 to provide oversight and guidance on data-related policies across the FDIC. The EDC plays a crucial role in implementing the Enterprise Data Governance Framework that facilitates the effective management of data holistically across the organization. The EDC meets once every two weeks to ensure that data initiatives are coordinated and support the FDIC's mission and strategic goals. The CDO chairs the EDC.
- **SEATAB.** The FDIC established the SEATAB in 2018 to serve as both a decision-making and an advisory body. The SEATAB establishes and approves IT technology standards, guidance, and strategy documents, and evaluates whether new technologies align to the EA and should be approved for use at the FDIC. In addition, the SEATAB performs technical assessments and provides recommendations regarding the implementation and use of new technologies. The Chief of the CIOO's Architecture and Design Section chairs the SEATAB, which meets twice per month.

A key component of this IT Governance Framework is ensuring adherence to federal mandates that govern how the FDIC manages information, engages with the public, manages risk, reports on performance, and ensures financial and operational accountability.

1.3. IT Workload Planning and Budget Formulation

The FDIC's Division of Finance (DOF) centrally administers the Corporation's annual workload planning process (including budget formulation and staffing requirements) and presents the agency's annual operating budget to the FDIC Board for approval. DOF also coordinates with the business Divisions and Offices to develop the agency's performance goals and measures, and monitors budget and spending variances throughout the year. In this role, DOF helps to ensure that IT investments align with business goals, objectives, and priorities, and that financial stewardship and accountability is maintained.

The FDIC's IT budget consists of four components: Investments, Initiative Projects, Ongoing Operations and Maintenance, and Receivership Funding. Investments are major, multi-year IT projects valued at $10 million or more that are subject to approval and oversight by the FDIC Board and the CIRC. The CIRC monitors these Investments and reports on their performance quarterly to the FDIC Board.

Initiative Projects consist of IT programs, projects, or activities that fall below the threshold for CIRC oversight (i.e., total projected cost of less than $10 million). Initiative Projects are non-recurring in nature (i.e., have a start and end date) and can span multiple years. The CIOO partners with the business Divisions and Offices to prepare a business case and cost estimate for each proposed Initiative Project and applies prioritization criteria to facilitate management review and approval of the projects. The CIOO uses multi-year business/IT roadmaps to plan new IT Initiative work.

Ongoing Operations and Maintenance consists of recurring IT work, software subscriptions, and equipment (including technology refresh initiatives). The CIOO works closely with DOF and other FDIC stakeholders to apply a structured methodology to build the Ongoing Operations and Maintenance budget. This includes developing workload-based justifications to support Ongoing Operations and Maintenance funding.

Receivership Funding consists of expenses to address IT issues related to the failure or near failure of FDIC-insured financial institutions and the management of receiverships established in connection with those failures.

The CIO coordinates with FDIC Division and Office Directors, including the DOF Director, to take a holistic view of funding requests when formulating the FDIC's annual IT budget, and to ensure the IT work aligns with the mission and priorities of the FDIC. The FDIC Board has responsibility for reviewing and approving the annual IT budget, and the FDIC Chairman approves IT-related Annual Performance Goals and FDIC Performance Goals. Throughout the budget year, DOF, the CIOO, and the governance bodies described above monitor and report on the performance of IT projects and spending relative to established plans.

2. IT Strategic Focus Areas

The CIOO has identified four Strategic Focus Areas that will guide the FDIC's annual IT planning and budget formulation activities and ensure alignment with the FDIC Strategic Plan. These four Strategic Focus Areas consist of Continuous Modernization, Operational Excellence, Workforce Enablement, and Data Management. Each Strategic Focus Area contains a set of Implementation Actions to guide the CIOO's work activities and track progress. As the FDIC works to revise its Strategic Plan, the CIOO will coordinate with business stakeholders to update and finalize the Implementation Actions.

2.1. Strategic Focus Area 1: Continuous Modernization

The FDIC relies heavily on technology to carry out its mission. As described below, the FDIC plans to continue investing in its IT infrastructure, cybersecurity and privacy programs, business systems and applications, data, and IT management practices to maintain a modern IT environment and improve the efficiency and effectiveness of business processes and operations.

Cloud Adoption and Technology Innovation

The FDIC is implementing a multi-year IT Modernization Program designed to bring the FDIC's IT environment into alignment with modern practices and standards in the IT industry, as well as key Federal priorities, including the Federal Cloud Smart Strategy and the Federal Data Strategy. Under the IT Modernization Program, the CIOO is working to modernize and migrate most of its information systems and data from legacy on-premises data centers to cloud technology platforms that offer enhanced IT capabilities, security, and resiliency. Cloud computing allows the FDIC to quickly and efficiently stand up IT solutions and only pay for those services that are needed.

The IT Modernization Program includes an objective to modernize the FDIC's bank examination business processes. To achieve this objective, the CIOO established a common cloud IT platform to host these processes. In June 2023, the FDIC completed the first major supervisory application modernization—the Framework for Oversight of Compliance and Community Reinvestment Act Activities User Suite (FOCUS)—on this platform and moved it into operation. FOCUS enhanced and replaced 11 legacy information systems and now provides examiners and bankers with an end-to-end solution that offers a significantly improved user experience and process efficiencies.

The FDIC is also undertaking a multi-year Investment project called Supervision360 to transition the agency's safety and soundness supervision-related systems from a legacy applications-based environment to a modern, cloud-based agile suite of applications. This effort will replace an estimated 18 legacy applications, reduce the amount of manual data entry surrounding supervisory activities, and expand the use of automation to identify emerging trends from examination activities, among other improvements. The CIOO plans to deliver Supervision360 on the same cloud platform hosting FOCUS, thereby enabling the reuse of the foundational IT infrastructure supporting these systems. The FDIC has implemented three releases of Supervision360 as of July 2025, and more releases are planned by the end of 2025.

Further, the FDIC will continue to explore how innovative technologies, such as AI and robotic process automation (RPA), can remove barriers and improve the efficiency and effectiveness of FDIC programs and operations. The FDIC recently established an enterprise governance framework to manage its AI projects and expanded the use of RPA to execute contracting actions that have historically been performed manually, resulting in significant efficiencies.

Implementation Actions

To maintain a modern IT environment, the CIOO plans to:

- Execute a phased migration of mission-essential and mission-critical systems to the cloud while identifying sustainable solutions for systems and services that remain on-premises;
- Decommission the back-up data center and reduce the size of the primary data center; and
- Make greater use of innovative technologies to automate manual business processes.

Cybersecurity Management

Every day, Federal agencies defend their networks, systems and data against sophisticated cyber threats from malicious actors. The FDIC therefore places a high priority on maintaining strong cybersecurity and privacy controls and practices. In its roles as an employer, deposit insurer, supervisor of state non-member banks, and receiver of failed institutions, the FDIC collects and maintains significant quantities of sensitive information, including personally identifiable information, confidential bank examination information, and sensitive financial data. The FDIC recognizes that it must maintain an effective information security program to mitigate the risk of cyberattacks that could compromise the agency's sensitive information or disrupt mission operations. The FDIC accomplishes this by aligning its IT investment decisions with agency and government-wide security and privacy goals and requirements.

The FDIC has established and implemented several information security program controls to protect its information systems and data. Such controls are consistent with Federal statutes, such as FISMA, and government-wide security policies, directives, and guidance issued by government organizations, including NIST, OMB, and the Department of Homeland Security. For example, the FDIC implements: identity, credential, and access management capabilities to ensure only authorized users, processes, and devices have access to the FDIC's IT resources; enterprise-wide continuous monitoring and threat detection to enable rapid identification and response to cyber threats; and plans, procedures, and technical measures to enable the recovery of mission-essential and mission-critical information systems, operations, and data after a disruption. The FDIC's 2025 Report on Cybersecuity and Resilience provides a comprehensive description on how the FDIC maintains and strengthens its information security program.

The FDIC's Information Security Program is also subject to regular audits conducted by the Government Accountability Office and FDIC Office of Inspector General (OIG). In its most recent annual evaluation, the FDIC OIG determined that the FDIC's Information Security Program is operating at a Level 4, "Managed and Measurable." In the context of the maturity model used by Federal

Inspectors General to assess Federal agency security programs, a Level 4 (out of 5) signifies that the FDIC's Information Security Program is operating at an effective level of security. The FDIC has maintained a Level 4 maturity rating for its information security program since 2021.

Implementation Actions

To ensure the FDIC continues to maintain effective information security program controls, the CIOO plans to continue ongoing efforts to:

- Enhance Identity, Credential, and Access Management cybersecurity controls;
- Implement a Zero Trust Architecture, with a focus on its five core pillars (i.e., identity, devices, networks, applications & workloads, and data); and
- Create and implement an enterprise Application Security (AppSec) Team to perform security testing of information systems to identify vulnerabilities.

2.2. Strategic Focus Area 2: Operational Excellence

The CIOO recognizes that it must continually assess and refine its operational processes, systems, and practices to ensure the consistent, reliable, and timely delivery of quality IT products and services. In this regard, the CIOO is working to expand and mature its use of modern systems development and delivery methods, such as Agile, Development/Security/Operations (DevSecOps), and product management. A number of industry recognized frameworks exist that define practices organizations can use in their operational IT environments to attain more predictable results and higher quality services to customers through comprehensive, systematic and integrated processes. The CIOO plans to leverage such frameworks to guide its efforts in achieving Operational Excellence. The CIOO will also continue to consider the use of inter-agency shared IT services where doing so is efficient, cost-effective, and consistent with the FDIC's needs.

Implementation Actions

To promote operational excellence in the IT program, the CIOO plans to:

- Mature the existing systems development life cycle model and associated DevSecOps practices;
- Enhance IT governance and oversight of IT projects;
- Assess the feasibility of adopting a product-based funding model;
- Optimize cost management practices;
- Ensure procurement strategies and standards effectively support the acquisition of innovative IT solutions from public and private sectors;
- Expand self-service capabilities, including through the Citizen Development Program;
- Strengthen IT asset management and software change management processes; and
- Replace, retire, or consolidate information systems, where feasible.

The CIOO is committed to continuously improving its operational processes, systems, and practices to ensure the integrity, security, and reliability of the IT services and products it provides to the agency, and to drive high user satisfaction.

2.3. Strategic Focus Area 3: Workforce Enablement

The FDIC recognizes that the success of its technology investments depends heavily on a workforce with the skills and competencies needed to deliver IT products and services that support the agency's business needs today and in the future. The FDIC places a high priority on attracting and retaining talented IT professionals with skills in the areas critical to achieving the FDIC's target-state IT environment, such as cloud architecture, cybersecurity, privacy management, agile development and delivery, product management, and strategic data management.

To guide its human capital management activities, the CIOO will work with the FDIC's Human Resources Organization to develop a comprehensive IT workforce planning strategy consistent with the concepts and principles in the Office of Personnel Management's (OPM) *Workforce Planning Guide*.[3] The IT workforce planning strategy will align with the FDIC's Workforce Optimization Initiative announced in 2025. The Workforce Optimization Initiative, which was undertaken pursuant to a Presidential Executive Order and related guidance issued by the OMB and OPM[4], aims to create a streamlined organizational and staffing structure and allow the FDIC to more efficiently accomplish its mission, without sacrificing the core functions Congress established in creating the agency.

Implementation Actions

To ensure effective workforce planning, the CIOO plans to:

- Continually assess workforce skills and competency needs and address gaps by attracting talent and retaining high-performing staff;
- Establish standardized position descriptions and career paths for staff to broaden their understanding of the CIOO and promote their advancement over time; and
- Promote continuous employee development in technical, management and leadership through training and partnerships with the FDIC's Corporate University and other academic and professional organizations.

[3] According to the *Workforce Planning Guide* (November 2022), workforce planning is the systematic process of analyzing and assessing to set targets to mitigate gaps between the workforce of today and the mission and human capital needs of tomorrow. Workforce planning helps to ensure the right people with the right skills are in the right positions at the right time to deliver results.

[4] Presidential Executive Order, entitled *Implementing the President's "Department of Government Efficiency" Workforce Optimization Initiative* (dated February 11, 2025); and OMB and OPM joint memorandum, entitled *Guidance on Agency RIF and Reorganization Plans Requested by Implementing The President's "Department of Government Efficiency" Workforce Optimization Initiative* (dated February 26, 2025).

By implementing effective human capital management practices, the CIOO can cultivate a high-performing workforce that consistently delivers quality, timely, and responsive IT services in support of the FDIC mission.

2.4. Strategic Focus Area 4: Data Management

The FDIC makes extensive use of data to drive strategic business initiatives and support informed decision-making. For example, the FDIC uses data to identify, analyze, and respond to current and emerging risks to insured financial institutions; price deposit insurance premiums; and perform pre- and post-resolution activities at financial institutions. The CIOO is committed to managing data as a strategic asset and advancing data management and analytics capabilities to support business analysis and decision-making.

To improve transparency, accountability, and effective data governance, the FDIC has implemented an enterprise-wide data governance framework that establishes clear policies and procedures for ensuring data health, effective metadata management, and robust data stewardship. The FDIC has also established a governance model specific to AI and machine learning, and has begun leveraging these technologies to power more sophisticated risk assessment and supervisory analytics. In 2024, the FDIC leveraged cloud-based machine learning and natural language processing tools built on a modern data orchestration platform to detect emerging risks, improve anomaly detection, and enable real-time analysis in the supervision program. The FDIC plans to pilot generative AI technology in 2025.

Embedded within its cloud migration and data modernization efforts, the enterprise data governance framework ensures a controlled, centralized catalog of FDIC data assets and clear data lineage tracking across cloud and on-premises systems. Consistent with relevant provisions of the Foundations for Evidence-Based Policymaking Act of 2018, the CIOO established the EDC and operationalized cataloging policies, which has enhanced data stewardship, traceability, and user trust in data throughout the agency.

Implementation Actions

To enhance data management, the CIOO plans to continue:

- Building a robust cloud data management and analytic capability;
- Ensuring relevant FDIC data are shared with the public in a timely manner; and
- Advancing a transparent, structured approach to govern the use of AI.

3. Enterprise Architecture

The CIOO developed the *2027 Target State Architecture* to guide the IT Modernization Program, support the achievement of this IRM Strategic Plan, and further the business goals and objectives in

the FDIC Strategic Plan.[5] The *2027 Target State Architecture* describes the technical IT components and capabilities required to support the business and serves as a roadmap for achieving the future-state IT environment. The CIOO uses the *2027 Target State Architecture* to inform investment decisions related to the IT infrastructure, information systems, and data ecosystem. The *2027 Target State Architecture* facilitates the achievement of operational efficiencies by reducing duplicate technologies, promoting the use of shared IT services, and reusing IT capabilities to the extent possible. The *2027 Target State Architecture* provides business value by establishing an enterprise-wide view of IT, and guiding the FDIC toward common goals and the adoption of simple, best-fit technical solutions that are cost-effective and align with business needs.

A key element of the EA program is the Business Capability Model, which offers a high-level representation of the fundamental capabilities required to fulfill the FDIC's mission. Through a collaborative process with all of the FDIC's Divisions and Offices, the CIOO has developed business unit roadmaps that link to the Business Capability Model and help guide IT investment decision-making. These roadmaps are consolidated into an enterprise Business Roadmap, which provides an integrated, multi-year view of milestones across the entire organization, ensuring the EA aligns with this IRM Strategic Plan.

4. Improving Services to Users

The FDIC leverages IT to support a broad range of users, including FDIC employees and contractors, Federal and state bank regulatory personnel, bankers, and members of the public. These users rely upon FDIC websites and information systems to access needed information and conduct important business activities, such as researching bank information, filing financial reports, paying deposit insurance assessments, making inquiries and complaints, and submitting bank applications. It is critical that the FDIC take a customer-centric approach in the delivery of IT services that support the agency's users. Such an approach includes measuring use and satisfaction of IT services through surveys, analytics, and other methods.

In 2024, the FDIC conducted several initiatives aimed at improving the public's experience in accessing digital content. One such initiative focused on the most publicly viewed parts of FDIC.gov where the agency provides resources and access to data for consumers, bankers, analysts, and other stakeholders. Such resources include electronic tools and searchable databases to perform analysis, and forms used to conduct business with the Corporation. The FDIC migrated FDIC.gov to a content management system, resulting in a more standardized look and feel for users. This change resolved numerous navigation inconsistencies and accessibility issues. In addition to enhancing FDIC.gov, the Corporation modernized the FDIC's BankFind Suite, which is a key resource for analyzing financial details and trends among FDIC-insured banks. The modernization enhanced users' ability to access and use public bank data.

[5] The CIOO is working to update the *2027 Target State Architecture* to incorporate the current Administration's priorities and guide the IT Modernization Program.

The FDIC regularly evaluates its existing and planned IT services through assessments and customer feedback to improve the user experience. For example, the FDIC maintains a Contact Center and Insurance Misrepresentation Portal, that allows the public to contact the Corporation with inquires, complaints, and questions.

5. Section 508 of the Rehabilitation Act

Section 508 of the Rehabilitation Act of 1973, as amended (Section 508), requires Federal agencies, including the FDIC, to provide employees with disabilities and members of the public with disabilities, access to information and data that is comparable to the access available to people without disabilities, unless doing so would create an undue burden on the agency. Section 508 applies to all Information and Communication Technology (ICT) products and services developed, procured, maintained, or used by the FDIC, including electronic files, videos, training materials, external and internal websites, systems, blogs, and social media.

The Section 508 Team within the CIOO has responsibility for reviewing all ICT for compliance with the statute. This team works with stakeholders throughout the agency to remediate instances of noncompliance and reports periodically to the CIO, CIO Council, and OMB on the FDIC's Section 508 compliance activities. The Section 508 Team also provides role-based training for employees with Section 508 responsibilities, including IT Project Managers, Internet Coordinators, and acquisition specialists. Such training serves to mitigate the risk of noncompliance, which can limit access for individuals with disabilities and expose the FDIC to legal and reputational risk.

6. Risk Management

The FDIC faces a variety of risks from both internal and external sources. In the context of IT, such risks include cyber threats, data breaches, and unexpected service interruptions that have the potential to negatively impact the FDIC's ability to achieve its strategic goals and objectives. The FDIC has established an Enterprise Risk Management (ERM) Program to effectively identify, assess, and address risks facing the FDIC. The FDIC Operating Committee, which is comprised of the leaders of the FDIC's Divisions and Offices, serves as the ERM oversight body. The FDIC's Chief Risk Officer (CRO), who leads the Office of Risk Management and Internal Controls, establishes agency-wide ERM policy and guidance, facilitates ERM implementation, and periodically reports on ERM activities to the Operating Committee.

As part of the ERM Program, the CIOO has developed and actively manages a Risk Inventory which describes the most significant IT risks facing the FDIC. The Risk Inventory contains the CIOO's assessment of the potential impact and likelihood of occurrence for each risk, as well as the associated mitigation measures. The CIOO has also established an information security risk management policy and supporting processes to ensure information security, privacy, and risk management activities are fully integrated into the system development life cycle. The risk management policy and processes comport with the NIST Risk Management Framework.

Additionally, the CIOO established the IT Risk Advisory Council (ITRAC) to monitor the IT and cybersecurity risks in the Risk Inventory and ensure these risks remain within established Risk Tolerance levels and FDIC's Risk Appetite statement.[6] The principal members of the ITRAC include the CIO, CISO, CDO, and CRO.

The CIOO recognizes that proactively identifying and effectively managing risks informs sound decision-making around business priorities and resource allocations and helps focus corrective actions on the most important risks.

7. Conclusion

This IRM Strategic Plan serves as a management tool to facilitate agency business and budget planning, ensure IT resources support strategic business goals and priorities, and promote IT performance measurement. Once the FDIC revises its Strategic Plan, the CIOO will coordinate with business stakeholders to update and finalize the Implementation Actions under each of the Strategic Focus Areas to ensure alignment with the Strategic Plan.

8. Open Data Plan

[6] The Risk Appetite statement defines the amount of risk the FDIC is willing to accept in pursuit of its mission.

Open Data Plan

August 2025

Federal Deposit Insurance Corporation
Chief Information Officer Organization

TABLE OF CONTENTS

ABOUT THE FDIC

The Federal Deposit Insurance Corporation (FDIC) is an independent agency of the U.S. government created in 1933 to maintain public confidence in the nation's financial system.

The FDIC:

- **Deposit Insurance:**
  Insures deposits at U.S. banks and savings institutions up to the legal limit (currently $250,000 per depositor, per ownership category at each FDIC-insured bank).
- **Examination and Supervision:**
  Examines and supervises state-chartered banks that are not members of the Federal Reserve System to ensure safe and sound operations and compliance with laws and regulations.
- **Bank Resolution:**
  Works to make large and complex financial institutions resolvable.
- **Receivership Management**:
  When a bank fails and the FDIC is appointed as receiver, it works to efficiently recover the maximum amount possible from the disposition of assets and pursuit of claims in the receivership.

To learn more about the FDIC, please visit https://www.fdic.gov/about

INTRODUCTION

The Federal Deposit Insurance Corporation (FDIC) plays a vital role in promoting public confidence and stability in the U.S. financial system through deposit insurance, supervision of financial institutions, and resolution of failed banks. As a steward of public trust and a key pillar of the U.S. financial system, the FDIC is committed to the principles of transparency, accountability, and public access to data. The FDIC's Open Data Plan has been developed in accordance with the OPEN Government DATA Act and aligned with the Federal Data Strategy.

FDIC's Open Data Plan provides a framework for publication of FDIC's data assets, ensuring data quality, engaging with stakeholders, and contributing to the government-wide Federal Data Catalog. Through this initiative, the FDIC seeks to maximize the use and reuse of its data to inform research, improve policy, and make FDIC data more readily available to the public.

OPEN DATA PLAN

In alignment with the Foundations for Evidence-Based Policymaking Act and the OPEN Government Data Act, agencies like the FDIC are required to implement open data principles that support transparency, accountability, and public engagement. The FDIC's Open Data Plan provides a structured approach for the handling of open data.

Open data is a cornerstone of good data governance, enabling the public, policymakers, researchers, industry, and the FDIC to access timely and trustworthy information. Open data informs internal decision-making and regulatory oversight, and enhances public understanding of financial systems and risks. Open data also supports evidence-based policymaking and empowers external stakeholders to better understand and participate in the policymaking process.

DATA COLLECTION AND INVENTORY

The FDIC's data management and governance practices call for the collection of metadata and other information about the data under its purview. As we standardize practices for data and data management, the Chief Data Officer Staff (CDOS) will continue to work with the FDIC to improve data health, and drive effectiveness and efficiencies.

Over the next year, the FDIC will:

- Finalize a comprehensive data inventory hosted in the agency's data catalog;
- Strengthen data literacy by promoting best practices for implementing open data standards and reinforcing the importance of using open formats;
- Advance open data capabilities by implementing clear rules and guidance for collecting and maintaining data in standardized and open formats under open licenses;
- Review existing data collection processes to identify and close gaps in open format adoption; and
- Evaluate tools that enable machine-readable data publication.

PUBLIC ENGAGEMENT AND COLLABORATION

The FDIC has a strong commitment to transparency, public engagement, and cross-sector collaboration. Through publicly available tools, reports, and downloadable datasets, the FDIC empowers stakeholders, including consumers, researchers, developers, and financial institutions, to better understand and participate in the U.S. banking system.

Central to this effort is the BankFind Suite, which includes tools and application programming interfaces (APIs) that enable users to search for and retrieve detailed information on FDIC-insured institutions. The Suite was modernized in 2022 to offer open API access without barriers. Since then, the FDIC has expanded opportunities for public interaction and data-driven collaboration, particularly among developers and analysts who integrate this information into broader financial tools and platforms. These enhancements demonstrate the FDIC's responsiveness to user needs and its investment in building a more open, reliable digital infrastructure.

Beyond technical access, the FDIC promotes public collaboration through regular stakeholder meetings, FOIA resources, and performance transparency initiatives. Targeted partnerships with external organizations are used to inform outreach initiatives, improve usability, and address issues related to access. Feedback mechanisms such as the CDO mailbox help inform decisions on data publication priorities.

These outreach efforts not only expand access to critical financial information, but also invite public input, foster dialogue, and build trust across stakeholders. Collectively, the Open Data Plan reinforces the FDIC's role as a collaborative partner in strengthening the stability, inclusiveness, and innovation of the financial system.

DATA ACCESSIBILITY AND USE MONITORING

All open data assets are published in machine-readable, non-proprietary formats and made accessible through portals like Data.gov and FDIC.gov. To improve visibility and discoverability, the FDIC will publish metadata related to our data assets to the Federal Data Catalog. This includes standardizing metadata tags and categorization to enhance search functionality for both internal and external stakeholders while aligning with federal cataloging requirements.

Data stewards throughout the FDIC help maintain the accuracy and quality of data assets under their purview. Internal tools will be used to regularly perform reviews of data assets as well as track dataset usage metrics and other measurements such as downloads, pageviews, and referral sources. These data will serve as a proxy measure for user demand and public impact.

DATA HEALTH AND IMPROVEMENT

To gauge the effectiveness of our information resources management and open data activities and ensure data health across the FDIC, we will establish indicators aligned with our strategic goals. Data health will be assessed across several dimensions, such as Persistence, Completeness, Discoverability, and Value. Best practices from across the FDIC will be synthesized into consistent guidance for data stewards and Division and Office stakeholders.

We are working to enhance lineage tracking, improve our data handling processes, and implement automated validations where appropriate. To promote continuous improvement, data stewards will be encouraged to participate

in regular reviews of our assets and evaluate metrics aligned to data health indicators. These regular evaluations will inform adjustments to strategies and ensure continuous improvement in managing our information resources.

PRIORITY DATA ASSETS AND FEDERAL CATALOG COMPLIANCE

To strengthen compliance with federal open data requirements, CDOS continues to coordinate closely with the FDIC's data stewards, Legal Division, FOIA program, and other Divisions and Offices, to ensure that public release of data assets are both lawful and appropriate. Prioritized data assets have been identified and captured in collaboration with data stewards. These assets and corresponding metadata are currently being loaded into the FDIC Data Catalog and will be loaded into the Federal Data Catalog by September 2026.

Open data processes and supporting technologies will be leveraged with our internal data catalog to automate and streamline the future publication of public data assets. These efforts are aligned with the requirements of the OPEN Government Data Act and OMB Phase 2 guidance. They are also designed to anticipate additional guidance on open data. These efforts ensure both our internal data catalog and submissions to the Federal Data Catalog conform to the Data Catalog Vocabulary (DCAT-US 3.0) metadata schema.

APPENDIX – GLOSSARY OF TERMS

- **Data** – Recorded information, regardless of form or the media on which the data is recorded. (44 U.S.C. § 3502(16))
- **Data asset** – A collection of data elements or data sets that may be grouped together. (44 U.S.C. § 3502(17))
- **Financial Data Transparency Act (**FDTA) – *Financial Data Transparency Act of 2022* (12 U.S.C. 5334)
- **Federal Data Catalog** – A centralized public online interface dedicated to sharing U.S. government data assets with the public; maintained by GSA and available through Data.gov. (Office of Management and Budget (OMB), *Phase 2 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Open Government Data Access and Management Guidance*, M-25-05 (January 15, 2025) (M-25-05))
- **Foundations for Evidence-Based Policymaking Act** - Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435, 132 Stat. 5529 (2019)
- **Machine-readable** - Data in a format that can be easily processed by a computer without human intervention while ensuring no semantic meaning is lost. (44 U.S.C. § 3502(18))
- **Metadata** - Structural or descriptive information about data such as content, format, source, rights, accuracy, provenance, frequency, periodicity, granularity, publisher or responsible party, contact information, method of collection, and other descriptions. (44 U.S.C. § 3502(19))
- **Open Data** – Publicly available data structured in a way that enables the data to be fully discoverable and usable by end users. (OMB, *Open Data Policy—Managing Information as an Asset*, M-13-13 (May 9, 2013))
- **Open format** – A file format for storing digital data where the format is platform independent and machine-readable and is maintained (A) at no cost to the public; and (B) with no restrictions on copying, publishing, distributing, transmitting, citing, or adapting such a format. (M-25-05)
- **Open Government Data Act** - Open, Public, Electronic, and Necessary Government Data Act, 44 U.S.C. §§ 3501 note, 3502, 3504, 3506, 3511, 3520 (2018).
- **Open Government data asset** – A public data asset that is-
    - Machine-readable;
    - Available (or could be made available) in an open format;
    - Not encumbered by restrictions, other than intellectual property rights, including under titles 17 and 35, that would impede the use or reuse of such asset; and
    - Based on an underlying open standard that is maintained by a standards organization. (44 U.S.C. § 3502(20))
- **Open license** – A legal guarantee that a data asset is made available-
    - At no cost to the public; and
    - With no restrictions on copying, publishing, distributing, transmitting, citing, or adapting such asset. (44 U.S.C. § 3502(21))
- **Public data asset** – A data asset, or part thereof, maintained by the Federal Government that has been, or may be, released to the public, including any data asset, or part thereof, subject to disclosure under section 552 of title 5. (44 U.S.C. § 3502(22))