Deloitte.

Gearing up for FDIC 370 compliance

System ready, data steady?

The Federal Deposit Insurance Corporation (FDIC), which provides the standard maximum deposit insurance amount (SMDIA) of $250,000[1] to depositors, recently issued new requirements for Insured Depository Institutions (IDIs). In the event of a failure, these requirements will provide depositors with prompt access to insurance coverage on their accounts. They will also resolve the failed institution in the least costly manner possible. The rule, called 12 C.F.R. Part 370 or "Recordkeeping for Timely Deposit Insurance Determination" Rule ("final rule"), issued on April 1, 2017, requires all Covered Institutions (CIs) with two million or more depository accounts to start complying with the final rule by April 1, 2020.

The final rule applies to domestic deposits only. The expectation is that, in the event of a failure, the FDIC will rely on the CIs to provide complete and accurate account and depositor information needed to determine the insurance coverage available to each depositor. To be compliant with the final rule, a CI must configure and implement IT systems to calculate insured and uninsured deposit amounts for each depositor by insurable category. If an institution fails and the FDIC takes over, a CI must be capable of:

- Calculating insured and uninsured amounts for each depositor
- Generating four output files: customer file, account file, account participant file, and pending file (collectively called the "output files")
- Putting a hold on uninsured amounts within 24 hours
- Verifying that for all deposit accounts, signed signature cards exist for each owner, and that signature cards exist for each co-owner for joint accounts

In addition, the final rule requires that a CI must annually certify that its IT systems are capable of providing the required information within 24 hours of its failure. This includes deposit information not held by the CI for accounts with transactional features.

To confirm compliance, the FDIC will conduct on-site inspections and testing of the CI's IT systems capability to calculate accurate deposit insurance coverage in the event of failure. Testing will begin no sooner than the last day of the first calendar quarter following the compliance date. It will occur no more frequently than on a three-year cycle thereafter, unless there is a material change to the CI's IT system, deposit-taking operations, or financial condition.

The final rule also calls for an accelerated implementation on a case-by-case basis where a CI:

- Has received a composite rating of 3, 4, or 5 under the Uniform Financial Institution's Rating System (CAMELS rating) in its most recently completed Report of Examination
- Has become undercapitalized, as defined in the prompt corrective action provisions of 12 C.F.R. part 325
- Is experiencing a significant capital deterioration, funding difficulties, or liquidity stress, notwithstanding the composite rating of the CI by its appropriate federal banking agency in its most recent Report of Examination

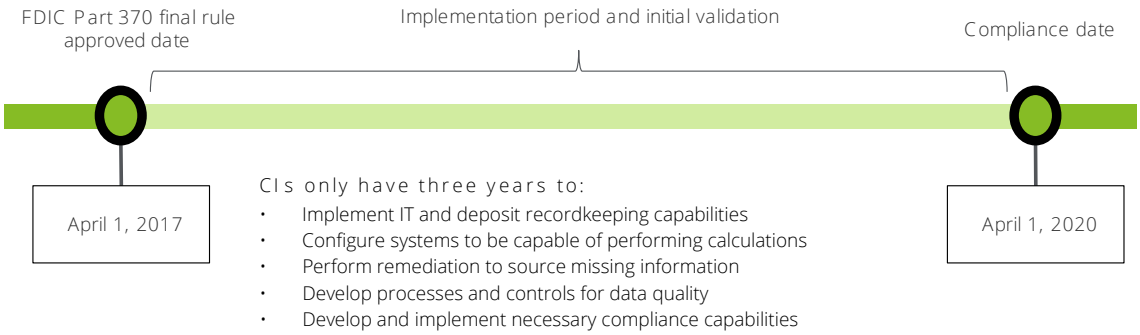
To meet these stringent data, technology, and compliance requirements, the FDIC has given CIs three years to comply with the regulation. Within this three-year implementation time span, CIs have the formidable task of addressing deficiencies in data quality, system functionality, and operational capacity to meet final rule requirements. They must also build a technology infrastructure capable of calculating deposit insurance and uninsured amounts on accounts as well as handling periodic testing and compliance certification procedures. In order to lead in the industry, executives must begin developing the strategy that will help them navigate the final rule requirements and timelines and identify opportunities to disrupt through innovation.

1 U.S. Code - Title 12 - Chapter 16 - Federal Deposit Insurance - Insurance Funds - 12 U.S.C. 1821(a)(1)(C), 1821(a)(1)(E).

2 Recordkeeping for Timely Deposit Insurance Determination, Federal Deposit Insurance Corporation, Final Rule, Effective April 1, 2017, https://www.fdic.gov/news/news/press/2016/pr16101a.pdf.

FDIC 370: At a glance (scope and timelines)

The final rule aims at improving resolvability of banks by allowing the FDIC to make deposit determination in a timely manner in the event of a bank's failure. It will also allow the FDIC to perform its mandatory least cost resolution test accurately.



The final rule improves upon previously issued FDIC regulation's Part 360.9 for deposit insurance determination deemed insufficient to mitigate the complexities that could arise from the failure of some of the largest IDIs.

	Part 360.9 requirements	New Part 370 requirements
Data gathering	Report only available data	Source all depositor data, even data currently not available
	Provide only insured amounts	Provide insured and uninsured amounts
Hold	Send standard format to FDIC	Create unique bank-developed form containing over 70 specific fields
	Hold insured deposit amounts at levels given by FDIC	Maintain data and perform analytics and calculations for provisional hold amounts

In accordance with the final rule, the FDIC estimates:

- The final rule will impact 38 IDIs, each having between 2 million and to 87 million deposit accounts
- CIs together have greater than $10 trillion in total assets and manage more than 400 million deposit accounts
- CIs will collectively spend more than $500 million to be compliant

Understanding the core rule requirements

The final rule contains specific guidance to ensure that, in the scenario of a failure, the FDIC can provide prompt payment of deposit insurance and resolve a CI in a manner that is least costly to the Deposit Insurance Fund (DIF). Large parts of its requirements anchor around the need for systematic data governance, enhanced data quality of deposit accounts, IT capabilities, and technology infrastructure. To meet the final rule requirements, CIs will need to demonstrate continuous progress and readiness, primarily in the following areas:

- **IT systems compliance testing and certification**
  The final rule requires CIs to certify annually that their systems are capable of calculating insurance coverage and uninsured amounts on deposit accounts. CIs are also required to certify that they can submit all information, required on deposit accounts with transactional features held in the name of a third party, to FDIC for deposit insurance coverage calculation upon the CI's failure. The chief executive officer (CEO) or chief operating officer (COO) must duly sign the certification before submitting to the FDIC. CIs will be required to ensure the data integration processes, customer and deposit information, insurance calculations, and output files generated are in continuous alignment with the requisitions of the final rule.

  In situations where a CI is experiencing rapid or significant changes to its deposit account volumes, operational processes, and deposit systems, the expectation for certification is more frequent. In addition to these periodic certifications, CIs can also expect to be tested for compliance by the FDIC once in a three-year cycle, or sooner if they have undergone consequential material, technology, or financial changes.

- **Comprehensive data management capabilities for domestic deposit accounts**
  The final rule, in conjunction with the IT Functional Guide[3] issued by the FDIC for Rule 370, gives paramount importance to data-centric activities—spanning across the life cycle of data sourcing, aggregation, standardization, accountability, data quality, data controls, and reporting—to make certain that CIs have complete and accurate information on domestic deposit accounts readily available. Under this mandate, it is essential for banks to have a single, consolidated view of not only the depositor but also the beneficiaries across the range of account types, deposit systems, and customer identifiers (e.g., SSN, TIN, etc.). An adept governance framework should be in place with clearly defined and documented standards, policies, ownership, and monitoring protocols shared between and agreed upon by various data producers and consumers.

  The stress that the final rule places on robust data management is also evident from the estimated implementation costs provided by the FDIC,[4] where 77.67 percent of the cost is attributable to data-focused tasks, including legacy data cleanup, data aggregation, data standardization, data extraction, quality control, and compliance. This amounts to greater than $370 million expected collective spend by CIs on improving the data management capabilities for insurance coverage calculations for accounts with more than $10 trillion in deposits at banks in the United States.

3 Information Technology Functional Guide, 12 CFR Part 370: Recordkeeping for Timely Deposit Insurance Determination, Version 1.0, Federal Deposit Insurance Corporation, April 2017, https://www.fdic.gov/regulations/resources/recordkeeping/documents/info-tech-func-guide-for-implement-part370.pdf

4 Page 34, Table 1 – Estimated Implementation Costs By Component, of final rule on Deposit Account Recordkeeping Requirements approved by FDIC on November 15th 2016, from the Information Technology Functional Guide for FDIC – Part 370 Recordkeeping.

- **Robust system architecture for sourcing, aggregation, calculation, and reporting**
  Providing deposit insurance coverage promptly is a key element of the final rule, for which the FDIC requires CIs to develop, configure, and maintain IT systems, enabling them to:

  – Standardize and aggregate deposit account details across multiple deposit systems
  – Calculate insured and uninsured amounts in each deposit account by ownership rights and capacity within 24 hours, with the ability to restrict access to some or all deposits while the FDIC determines the insurance coverage
  – Process and generate required data output files and metrics

  The final rule also contains explicit requirements on the structure, format, and content of the output files, along with the interdependencies they need to satisfy. As previously stated, a CI needs to ensure it can provide these output files within 24 hours after the FDIC takes over the CI.

Key challenges and other considerations for CIs

Taking into account the massive deposit account volumes, disparate customer onboarding procedures, and relatively tight timelines imposed by the FDIC to conform to the final rule requirements, it will be important for CIs to ensure that senior management understands the project complexity and allocates adequate time and resources to achieve successful completion. This will require coordinated efforts to overcome evident data quality issues, strategic planning to prevail over current technology limitations, and tactical decision making to circumvent immediate operational challenges, some of which are summarized below:

- **Missing single and complete view of a customer**
  Achieving a consolidated, single view of customer data has been the elusive holy grail for many banking organizations. The final rule has given a renewed impetus to this endeavor as the basis for calculating insured and uninsured amounts for deposit accounts by ownership rights and capacity. Banks have made modest progress in this direction—partly because of improved customer onboarding processes as required by past regulations (such as KYC, AML, FATCA, etc.). However, the challenge of compiling, aggregating, and reconciling across existing and new customer accounts, multiple deposit product types, mismatched unique customer identifiers across systems (e.g., SSN, TIN, system generated ID, etc.), error-prone manual processes, and electronic/physical documents still largely remains.

- **Integrating multiple deposit systems and sources**
  As banks have grown, organically as well as from mergers and acquisitions, there has been an increasing need to unify and harmonize both account data and business processes across deposit systems and applications. Already a task of formidable magnitude, it is further compounded by the fact that the platforms to be synchronized can vary from cloud, mainframe, proprietary, and open source to bespoke vendor-specific technologies. Beyond the underlying platforms, it is also not atypical to observe such nuances as unstructured formats, inconsistent data definitions, and conflicting ownership issues across data sources for deposit accounts.

  CIs should consider streamlining their IT systems and operational processes as part of their implementation program for final rule compliance. Beyond the reporting data warehouse and data lakes they may already have, developing a central deposit calculation system and replacing paper signature cards with electronic ones are worth serious contemplation as next steps.

- **Calculating complex insurance scenarios expeditiously**
  As mentioned earlier, one of the cornerstones of the final rule is that it requires each CI to calculate the insured amount by depositor as defined by Part 330, Deposit Insurance Coverage, which contains multiple combinations. To add to the complexity of managing insurance scenarios, in the event of failure, the IT systems of the CIs are required to:

  – Aggregate data from multiple source systems
  – Complete these calculations in less than 24 hours
  – Generate four output files with more than 70 fields and transfer them to the FDIC

- **Lack of or insufficient data management capabilities**
  Final rule requirements around complete and accurate data of a depositor and deposit accounts make it crucial for the CI to reexamine its existing data management capabilities. The FDIC has issued an "Information Technology Functional Guide" to assist the CIs in implementing compliant systems, with directions the CIs will need to follow to ensure data required by the final rule is fit for its intended use. Those directions include:

  - **Data lineage.** Identification of critical data elements (CDE) for depositor, account, and balance information as needed for the output files, tracing data movement from various source systems to target state (as stated in section 6.1 Data Movement).
  - **Data governance.** Designing and developing policies and standards (as stated in section 6.2.1 Data Quality Policies and Standards) as well as clearly defined roles, responsibilities, accountabilities, and oversights (as stated in section 6.2.2 Data Quality Accountability).
  - **Data quality.** Ongoing profiling and assessment of data, analysis/prioritization of issues, and established remediation strategies (as stated in section 6.2.3 Data Quality Assessment and Remediation).
  - **Data controls.** Control reports for data monitoring and reviewing reconciliation effectiveness, such as three-way reconciliation between general ledger, deposit systems, and output files (as stated in section 6.3 Control Reports).

  Based on the final rule requirements, there is additional data required for up to 70 fields, which may not all be readily available from information stored on paper documents and may require customer input.

- **Addressing pass-through deposit insurance requirements**
  In addition to capturing the required information to determine insured and uninsured status contained within the CI, there is also a requirement for information on deposits held in the CI by depositors through financial intermediaries outside the CI. These are referred to as "pass-through" deposits, such as brokered deposits. This also includes deposits held in trust through affiliates and third-party entities and means the CI will need to work with these outside entities to achieve compliance. The challenge with this deposit relationship is that the CI does not directly control the required information. This means there will likely be some variability in practices and controls along with the need to address potential information gaps. Fortunately, there are alternative recordkeeping requirements for many of these accounts that result in less required information. However, there is still a minimum requirement, including the need for a unique identifier and reason for holding the accounts in a pending file.

  Another challenge posed by pass-through deposits is identifying accounts with transactional features within the 24-hour time requirement should a CI fail. While a CI does not have to calculate the insured and uninsured balances on a daily basis, it is required to have the ability to calculate those balances on any given day. To maintain this capability, the covered bank will need to make sure the required information is available and that the holder of that information outside the CI maintains it so it is accessible, if necessary, within a 24-hour period. To ensure this capability is maintained, it is covered as part of the annual certification process. This means the CIs will need to have processes and controls in place for third parties that provide pass-through insurance. There are certain accounts with transactional features that fall outside the certification process, such as those maintained by a mortgage servicer, since those types of transactions are less sensitive to temporary delays in access.

Understanding your current state baseline is imperative

Getting a head start with the strategy and implementation approach will be critical for CIs to comply with the final rule requirements and timelines. This is the right time to start the evaluation of current system capabilities, data availability, and quality of the deposit accounts, which can enable CIs to identify pronounced gaps and shortcomings against the final rule requirements. Such an analysis can help to prioritize and remediate issues and roadblocks to the final rule readiness and implementation program.

To plan for next steps, CIs should ask themselves the following questions:

- Have we established a program governance process for ongoing management of project scope, activities, deliverables, timelines, and communications?
- Have we identified stakeholders, customer accounts, deposit systems, and business processes that fall within the scope of the final rule?
- Does our current data management framework meet the data requirements of the final rule, such as validating the completeness and accuracy of data with business rules and monitoring data quality on an ongoing basis?
- What are some of the high-impact deposit accounts for FDIC reporting with potentially incomplete account data?
- What approach should we adopt to identify and link deposit account holder across various deposit product types and deposit systems?
- Have we identified all deposit account information (pass-through) that resides outside the bank, along with the entity responsible for that information? In addition, is there an established process to ensure that data will conform to the rule requirements?
- What processes are required to prioritize deposit accounts, transaction versus non-transaction, to plan for staffing and resource allocation?
- Have we engaged the legal and compliance teams to review contract language for deposit accounts?
- What is the process to review signature cards for existing accounts and flag those that are missing customer information?

Why Deloitte?

Deloitte is well-positioned to assist with this initiative. We bring both depth of regulatory insight and, equally important, considerable experience working with executives to help them implement similar regulatory requirements that call for system and data transformation. Our strengths include:

- **Extensive regulatory experience** (specifically with the FDIC) and ongoing engagement with regulators means we can provide the regulatory insights needed to help you navigate the obstacles that come with complying with FDIC Part 370.
- **Working closely with former FDIC leads as independent advisors**—with experience relating to deposit insurance determination—for implementation guidance based on their experiences with related aspects of the final rule, such as data capture process, provisional hold rule, IT system development, and deposit insurance coverage estimations.
- **A dedicated team** with a history of helping large and complex financial institutions to efficiently implement strategies to meet new regulatory requirements, including:
  - Establishing appropriate programs and governance and conducting gap assessments
  - Formulating strategies for remediation, design, and implementation of IT and data infrastructure
  - Incorporating new capabilities seamlessly into daily operations

  We have a reputation for providing the appropriate strategy that helps large CIs meet regulatory requirements and bring significant value to the business in a timely fashion.
- **Specialized risk data management practice** with a demonstrated track record of assisting and effectively conducting major enterprise-wide projects and data-centric engagements at financial institutions, using tools and accelerators that are based on structured templates and straw-man models, to cut down on learning curves and expedite delivery.
- **Familiarity with system capabilities assessment**, required by various regulatory bodies, such as the Federal Reserve, Securities and Exchange Commission, Internal Revenue Service, etc., through issuance of various regulations impacting technology infrastructure. Deloitte routinely helps clients perform current-state and system-impact analysis for regulatory requirements, in addition to conducting vendor assessments.
- **Leading technology innovation and supporting infrastructure**, which includes facilities like the Deloitte Greenhouse Lab, to assist with designing and implementing enterprise-wide data architecture solutions capable of managing large data volumes from multiple source systems, similar to the type of solution needed to comply with FDIC Part 370.

Deloitte's Risk Data Management (RDM) practice and the Center for Intelligent Automation and Analytics (CIAA)

Deloitte has a dedicated RDM practice to assist executives with leveraging data as a strategic asset and using it for competitive advantage. Deloitte also has a CIAA group, which serves as a catalyst for bringing intelligent automation and analytics solutions to the marketplace, with a specific focus on:

- Enhancing capabilities in the areas of robotic process automation (RPA) and cognitive intelligence
- Providing industry-leading thinking in automation through the development of new technologies and use cases

Effectively implementing requirements for the final rule will require CIs to have sustainable and efficient data governance and data quality processes. Deloitte's CIAA can help CIs navigate their implementation journey to explore areas of automation, where it may be possible to disrupt through innovation and replace or improve upon the manual steps or existing data extraction, aggregation, and standardization activities with RPA and/or cognitive intelligence tools. Deloitte's CIAA can also work with executives to help them lead by identifying opportunities to realize cost reductions with better customer insights, improved monitoring abilities, and real-time consolidated views of insured as well as uninsured balances.

FDIC Part 370 Rule CoE leadership

Olga Kasparova
Managing Director
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 617 437 2812
okasparova@deloitte.com

Michael Quilatan
Managing Director
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 212 436 2230
mquilatan@deloitte.com

Monica O'Reilly
Principal
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 415 783 5780
monoreilly@deloitte.com

Laura Survant
Partner
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 213 688 4123
llsurvant@deloitte.com

Senior Advisors

John Corston
Ex-FDIC, Independent
Advisor to Deloitte & Touche LLP
+1 212 436 2388
jcorston@deloitte.com

Joseph Fellerman
Ex-FDIC, Independent
Advisor to Deloitte & Touche LLP
+1 571 271 2181
jfellerman@deloitte.com

Authors

Mike Thakkar
Senior Manager
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 212 436 5544
mithakkar@deloitte.com

Ravikiran Shetty
Senior Manager
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 470 362 4531
ravishetty@deloitte.com

Sanny Kumar
Manager
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 973 602 5905
sannkumar@deloitte.com

Deloitte.