An Integrated Approach to Adopting FDIC 370 with Oracle

On April 1, 2017 the Federal Deposit Insurance Corporation (FDIC) released its final rule on "Recordkeeping for Timely Deposit Insurance Determination" or 12 CFR Part 370 (commonly referred to as FDIC 370). The intent of the rule is to facilitate the prompt payment of deposit insurance after the failure of a depository institution. Prompt payment is believed by the FDIC to be important to maintain public confidence in the banking system, avoid broader disruption to the financial system, and to enhance the franchise value realized under resolution by expanding the range of available options.

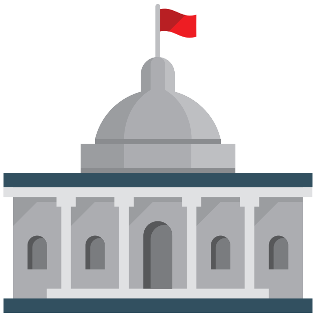
The rule is another example of a regulation that requires institutions to have greater centralization and control of critical customer, product and transaction data with more frequent processing – similar regulations (think 2052A/B, CECL, etc.) have caused many institutions to consider more integrated finance and risk platforms and operations. Although banks have had to comply with FDIC 360.9, the FDIC introduced FDIC 370 to put greater ownership on insured depository institutions (IDIs) to aggregate and calculate insurance payouts to depositors during a resolution. The stimulus for this change was the FDIC's experience with the complexities present at large institutions caused by the number of deposit systems, the lack of standardized data, and the volume of records.

To meet this end, the final rule defines new data management, deposit insurance computation, and governance requirements for covered institutions (defined as IDIs with greater than 2 million deposit accounts). These requirements will force banks to review systems, data, and management of their insurance-eligible lines of business from customer on-boarding all the way through to reporting – and the deadline of 2020 is rapidly approaching. The provisions of the rule discourage the implementation of "point" solutions through restrictions on manual processes and mandatory reconciliations with the general ledger and other filings.

REQUIREMENTS AND CHALLENGES

The final rule requires Covered Institutions (Cis) to configure and implement information technology systems capable of calculating the insured and uninsured amounts for each deposit account, producing four required output files, and placing a hold on insured amounts within 24 hours of bank failure. IDIs must certify annually that their data is complete and accurate, and that their systems are prepared to provide the required information within 24 hours.

The required output files comprise over 70 data fields, all of which are mandatory (unless the account qualifies for alternative record-keeping). This is in stark contrast to the requirements under part 360.9, which requires IDIs to complete a standard form on a 'best efforts' basis only. Furthermore, the new rule requires CIs to assign each depositor to one of 14 Ownership Rights and Capacity (ORC) codes and calculate insured amounts themselves. Insured amounts are calculated by the FDIC under part 360.9.



FDIC 370 Requirements

IDIs must be able to:

- Calculate the insured and uninsured amounts for each deposit account
- Assign each depositor one of 14 ORC codes and calculate insured amount
- Produce four required output files – comprising more than 70 data fields
- Place a hold on insured amounts within 24 hours of bank failure
- Certify annually that insured account data is complete and accurate and that systems can provide required data in 24 hours
- Reconcile data at the account level with the general ledger and the systems of record

FDIC 370 also specifies that CIs implement processes that include reconciliation to both the GL and the systems of record at the account level. An overview of such reconciliations, certain data quality controls, and a summary of various deposit measures (balance, count, etc.) by ORC must be reflected in the required Summary and Control management reports. The FDIC has yet to specify if there will be any requirement for periodic submission of the data files or other reports to the FDIC in the ordinary course of business. After April 1, 2020, IDIs will be subject to on-site inspections and testing of their systems no more frequently than once every three years unless there is a material change to their deposit operations or financial condition.

System Integration

As a byproduct of their histories and growth processes (for example, mergers and acquisitions), CIs today typically manage multiple disparate deposit systems of record and often more than one KYC or customer database. These multiple systems can be distributed across different legal entities, feature differing data definitions, and reflect varying customer identifiers and/or naming conventions. All of the aforementioned factors must be surmounted to create the unified consolidated view of each depositor required by FDIC 370.

Forward-looking CIs may view FDIC 370 as an opportunity to drive the digitization of their customer onboarding processes and to modernize their core banking platforms. Increased efficiency and elimination of physical records/manual processes allows a more nimble environment capable of adapting to new products and/or growth. The data requirements of FDIC 370 overlap to a large degree with those of Know Your Customer and Anti-Money Laundering, making the potential benefits of an integrated solution clear to all. Similarly, the potential benefits of a unified platform allowing the integration of deposit insurance calculations with FTP, profitability, and/or liquidity management processes.

Data Quality & Completeness

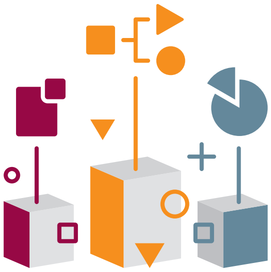
As described above, the final rule requires CIs to attest to their ability to produce reports with the 70+ mandatory fields populated for all depositors. This presents a significant challenge for CIs as a portion of the required data elements may be optional in their existing deposit/KYC systems, or even may currently only exist in archived physical documentation. Furthermore, any manual processes related to customer on-boarding or the deposit-taking business of the CI will need to be reviewed and addressed to eliminate errors. In addition to ensuring the completeness of data elements, CIs will need to put in place new normalization/standardization measures to ensure the consistency of data (for example, the same ID for every instance of a specific counterparty) as this has a direct impact on the insurance calculations. Due to the data governance and control requirements of FDIC 370, manual remediation of data gaps is not an option. Lastly, the capture of required data elements for deposits held by CIs through other financial intermediaries (e.g. brokered deposits) is expected to be a formidable task for CIs as they do not 'control' the required information in such cases.

Technical Burden

As mentioned earlier, FDIC 370 requires that CIs implement systems and processes capable of performing the insurance calculations and producing the required reports within 24 hours of failure. While the ORC assignment logic and insurance coverage calculations do not involve any stochastic modeling, they are sufficiently complex to make the required timing highly demanding for any automated solution, especially when the number of deposit records impacted can number anywhere from 2 million to 87 million.

Data Governance & Control

The final rule outlines specific data management requirements to ensure that data is fit for the use of FDIC 370. Among those requirements are data lineage, data quality standards and accountability, data governance policies, and data controls. Many CIs may have begun projects covering some of these elements as part of their BCBS 239 or CCAR attestation initiatives, but it is unlikely that their deposit systems and processes have been a focus of these efforts.



Expanded Data Management

FDIC 370 introduces new standards and requirements for:

- Data lineage
- Data quality and accountability
- Data governance policies
- Data controls

ORACLE FINANCIAL SERVICES ANALYTICAL APPLICATIONS' SOLUTION

The Oracle Financial Services Analytical Applications (OFSAA) solution empowers financial services organizations to manage and execute compliance in a single integrated environment. It automates end-to-end processes from data capture through reporting with industry-leading solutions. The Oracle solution includes 4 components:

Data Aggregation

The bedrock for OFSAA solutions, the Oracle Financial Services Data Foundation (OFSDF) leverages Oracle's financial services domain expertise to deliver a ready-to-deploy, end-use proven, practical platform for managing analytical application data. The OFSDF staging and results tables were designed to hold deposit data across a broad range of account types including Savings and Checking accounts, Time Deposits, CDs, NOW accounts, Money market accounts, and Brokered Deposits, and have been extended to capture additional fields relevant to FDIC 370. Additionally, OFSDF's party tables support the data elements required to assign the 14 different ORC codes defined under FDIC 370. Furthermore, Oracle Financial Services Data Integration Hub has metadata-driven data movement capabilities, allowing the movement of data from disparate customer information systems, deposit systems and general ledgers to the Oracle Financial Services Data Foundation. Data lineage, access controls, versioning, and audit logs are all native functionality to the data foundation and meet the requirements of FDIC 370. Institutions that have adopted OFSDF for other regulations have much of this data already captured with the appropriate integration and daily processing for FDIC 370.

Data Validation & Governance

The Oracle Financial Services Analytical Applications Infrastructure (AAI) has pre-built data quality checks specifically for the data elements required for FDIC 370 calculations and reporting. AAI supports all of the OFSAA solutions and provides close to 2,000 data quality checks out-of-the-box including numerous checks related to the data elements related to the prior deposit insurance rule (FDIC 360.9). AAI also supports the creation of logic within validations to populate missing values or to normalize data to ensure consistency. Oracle Financial Services Data Governance Studio (DGS) offers the capability to create the FDIC 370 Pending file (a file containing accounts lacking the full complement of data elements) and the associated remediation workflow and task assignments. The Oracle Financial Services Reconciliation Framework is a core component of the OFSAA platform and is designed to handle reconciliations between sourced data and corresponding GL accounts at multiple levels of granularity. Any supplementary reconciliations between FDIC 370 and other reports (e.g. Call Report, 2052a, FR2900) that customers may desire can be configured using DGS. Furthermore, OFSAA's solution offers control reports and a data glossary in-line with regulator expectations.

Insurance Calculation

Oracle's solution is pre-configured with a set of business rules to assign one of the 14 ORC codes to each insurance-eligible account based on the detailed data related to the owner, beneficiary and account type loaded to OFSDF. Similarly, the computation algorithm defined by the FDIC to calculate insured and uninsured amounts for each account/account owner across ORC types is pre-built within the OFSAA solution. In addition to the deposit insurance determination, OFSAA's solution is designed to apply the uninsured amount across accounts according to the FDIC's liquidity priority order.

Reporting & Analytics

Out-of-the-box, the OFSAA FDIC 370 solution supports the creation and submission of the four required data files (Customer, Account, Account Participant, and Pending) in addition to the Summary and Control reports defined in the Information Technology Functional Guide provided by the FDIC. Moreover, the OFSAA solution provides an FDIC 370 management dashboard through the Oracle Financial Services Data Governance Studio allowing insight into trends and variance of insurance/uninsured amounts at multiple levels of granularity, as well as various concentration analyses. Lastly, Oracle's business intelligence suite allows the creation of custom and/or ad-hoc reporting across any of the FDIC 370 data within the data foundation.

WHY ORACLE?

Data Management Expertise

Oracle offers the best-in-breed data management solution for the financial services industry and the data integration, normalization and validation requirements of FDIC 370 play directly to OFSAA's strengths. In its final rule, the FDIC provides implementation cost estimates that indicate it expects over 77% of expenditures on FDIC 370 to be related to data-focused tasks. In stark contrast to its point-solution/last-mile competitors, end-to-end data management is one of OFSAA's core competencies.

Cost Reduction

FDIC 370 presents an opportunity for CIs to address the modernization and automation of their deposit taking lines of business. It is commonplace for these businesses to rely heavily on disparate and/or outdated systems in additional to manual processes. The data accountability and control requirements of FDIC 370 will require CIs to address such issues with the benefit of eliminating inefficient or redundant processes and systems. Furthermore, an integrated solution such as Oracle's affords incremental efficiencies by leveraging existing infrastructure and allowing the retirement of legacy deposit insurance calculation engines.

For customers who have adopted OFSAA solutions for other use-cases, there is potential for significant savings from the re-use of existing infrastructure. System integrations, data sourcing, reconciliations, and data validations can all be leveraged for the FDIC 370 solution as opposed to starting from scratch. In particular customers of the OFSAA Regulatory Reporting and Liquidity Management solutions will see overlaps between their data already sourced and FDIC 370.

Enhanced Business Intelligence

By gathering depositor data across all systems and products into a consolidated, normalized view CIs will be able derive insight into customer behavior that was previously unavailable. This enhanced understanding can be leveraged by the CI to inform pricing decisions or identify cross-sell opportunities. Similarly, the aggregation of account data and standardization of customer/beneficiary data will improve Anti-Money Laundering monitoring through the illumination of heretofore undiscovered linkages and/or activity. Lastly, the enhanced view of insured/uninsured deposit balances afforded by the FDIC 370 solution can be utilized to augment the CIs liquidity management framework.

CONCLUSION

CIs need a clear strategy to address the Rule requirements; the most challenging requirements will take significant time and coordination. Covered Institutions only have three years to:

- Implement IT and deposit recordkeeping capabilities
- Configure systems to be capable of performing new detailed calculations
- Perform remediation to source missing information
- Develop processes and controls for data quality

By engaging with a technology provider like Oracle, who can offer you a full end-to-end solution, will only put you in a better position to be compliant by 2020.

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com/oracleFS facebook.com/oracleFS twitter.com/oracleFS

Integrated Cloud Applications & Platform Services

Oracle is committed to developing practices and products that help protect the environment