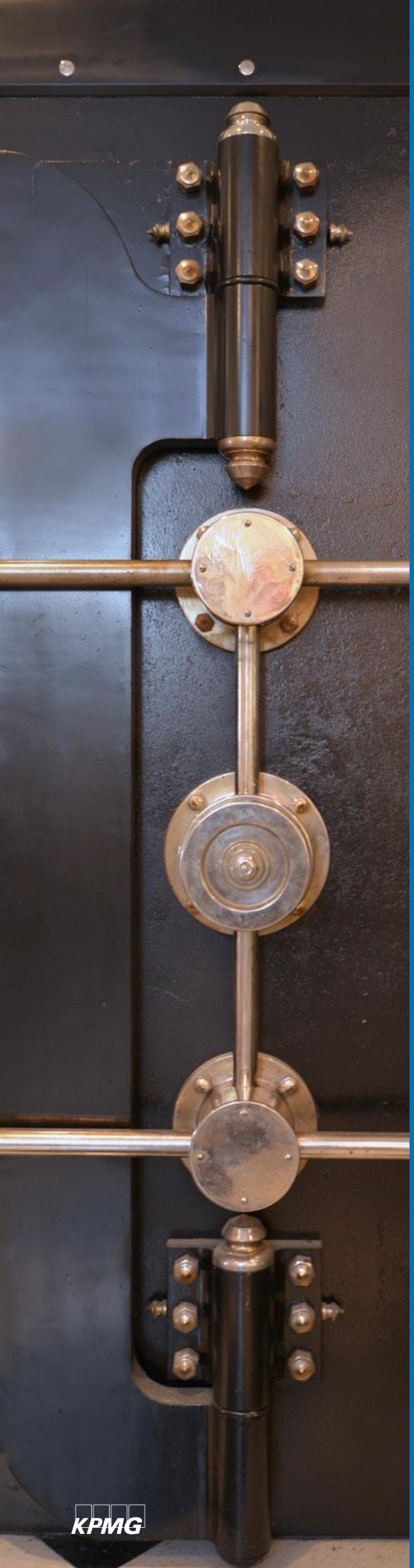
KPMG

The final say

Preparing for the FDIC's final deposit insurance recordkeeping requirements

kpmg.com



The Federal Deposit Insurance Corporation's (FDIC) new recordkeeping requirements have shifted the responsibility for determining deposit insurance coverage from the FDIC to those insured depository institutions (IDIs), or Covered Institutions (CIs), subject to 12 CFR Part 370 (Part 370 or the Rule). Referred to as the "Recordkeeping for Timely Deposit Insurance Determination" rule, Part 370 is intended to ensure that depositors have prompt access to their insured funds in the event of a large bank failure.

The Rule requires CIs to configure their information technology (IT) systems to capture, assess, calculate, and report deposit insurance coverage. While there are opportunities to leverage data transformations required by other regulations, Part 370 introduces significant complexities that will fully engage CIs over the allotted three-year implementation period.

Specifically, CIs must address the treatment of products with deposit characteristics, unrefined and/or incomplete customer data that may not have been effectively captured at account establishment, a 24 hour window to substantiate insured versus uninsured amounts, and the integration of multiple internal and external sources.

KPMG

The rule in summary

Part 370 shifts the focus of CIs from providing available data on insured accounts to performing the determination of insured deposits based on underlying bank data. By April 2020, IDIs with two million or more deposit accounts must maintain complete and accurate records regarding the ownership and insurability of all domestic deposit accounts. CIs will be required to:

1. Maintain complete and accurate information in accordance with the guidance stipulated by the FDIC to determine deposit insurance coverage for the 14 distinct account ownership categories set out in 12 CFR Part 370.
2. Configure IT systems capable of:
   - Calculating the amount of insured and uninsured funds for each deposit account within 24 hours of a failure;
   - Generating and retaining output records in the FDIC-specified format (as outlined in the Rule), including 77 fields across 4 prescribed reports;
   - Restricting access to deposits in a deposit account until the FDIC completes its insurance determination for that account (using the CI's IT system of record); and
   - Debiting from each deposit account the calculated uninsured amount.
3. Establish a comprehensive data management capability. The Rule borrows from other regulatory frameworks (e.g. BCBS 239) to encourage a robust set of data governance policies, standards and procedures.
4. Submit annually to the FDIC a certification of compliance and a deposit insurance coverage summary report.

CIs Defined. The Rule defines CIs as any IDI that has two million or more deposit accounts during the two consecutive quarters preceding the effective date of the Rule, which is April 1, 2017, or thereafter. CIs are provided three years from the date they qualify as a CI to comply with the provisions of the Rule, though the FDIC may accelerate this timeframe on a case-by-case basis. If a CI has fewer than two million deposit accounts during three consecutive quarters it may request relief from Part 370.

Understanding the complexities for CIs

Part 370 introduces considerable challenges compared to the requirements of 12 CFR Part 360.9 (the FDIC's prior rule for deposit insurance determination). CIs will need to take a more holistic view of customer data points, integrate data across a number of deposit systems and third party platforms, assess insurance for products with complex terms and conditions by customer, swiftly substantiate insured verses uninsured accounts, and implement a comprehensive data management framework.

KPMG

Evolution of insurance determination

12 CFR Part 360.9, Large-bank Deposit Insurance Determination Modernization, was introduced in 2008 as a step toward ensuring prompt deposit insurance determinations at large IDIs. It applies to IDIs with at least $2 billion in domestic deposits and at least 250,000 deposit accounts or $20 billion in total assets. It requires these institutions to:

— Maintain the technological capability to automatically place and release provisional holds on deposit accounts; and

— Transfer specific data to the FDIC in a prescribed form.

The FDIC has concluded that the standard data sets and other requirements of Part 360.9 are not sufficient to mitigate the complexities presented in the failure of the largest institutions.

CIs will be released from the provisional hold and standard data format requirements of 12 CFR Part 360.9 upon submitting the compliance certification required by Part 370.

Creating a holistic view of the customer

Many banks have made headway in achieving the sought after holistic, single view of the customer. However, Part 370 adds to this challenge of compiling, aggregating, and reconciling across existing and new customer accounts, external participants (e.g., federal government agencies), multiple deposit products, and mismatched unique customer identifiers across systems (e.g., SSN). The biggest hurdles will continue to be poor data quality and integration challenges, which, more than ever, will require CI's to tactically manage their customer master data.

Integrating deposit systems

Part 370 will increase the need for CI's to synchronize both account data and business processes across deposit systems and applications. In order to do this in the most effective manner, CIs should consider streamlining their IT systems and operational systems. Additionally, many banks will need to synchronize the multiple platforms (cloud, mainframe, open source, etc.) they use. The challenges of integration for CI's will not stop there. Unstructured data, inconsistent data definitions/reference data and conflicting data ownership across the data sources for deposit accounts will make this task demanding and potentially complex.

Dealing with complex deposit determination algorithm requirements in an expedited timeframe

Questions such as "How are gift cards handled" and "What about the original deposit to secure a credit card" will arise. CIs will need to consider the structure of the products that they offer as well as the language (terms and conditions details) used in customer agreements and other documents used in the establishment of new accounts. Justifying why certain deposits have been determined uninsurable will be critical in order to satisfy FDIC needs while ensuring premium payments are accurate.

Cost of compliance

CIs will need to configure IT systems and processes to be capable of annually certifying the accuracy of deposit insurance calculations in the event of a large bank failure. The cost to implement enhanced technology and processes could result in significant investment. To reduce the cost of compliance, banks could look to leverage scalable cloud or virtual technologies aligned with their overall technology and business process strategy.

Extending data management

Banks have implemented data governance offices of varying levels of maturity, as well as data quality remediation programs, however CI's will need to take a closer look at their existing data management capabilities. Part 370 explicitly requires complete and accurate data of a depositor and deposit accounts. The Rule places specific emphasis on:

— Identifying critical data elements needed for the output files;

— Tracing movement of data from various source systems to final reporting output;

— Designing and developing policies, procedures and standards as well as clearly defined roles, responsibilities, accountability, and oversight;

— Establishing a comprehensive data quality assessment to determine gaps and initiating robust remediation programs as required; and

— Developing control reports for data monitoring and reviewing reconciliation effectiveness, such as three-way reconciliation between general ledger, deposit systems, and output files.

How do you respond?

IDIs impacted by Part 370 will need to assess current capabilities against the requirements of the final rule and develop a plan for remediation in 2018. Given the likely need for enhancements to existing processes, technology, and data requirements, remediation activities will need to be coordinated with other priorities and implemented with sufficient time to test operational effectiveness in 2019 across the three lines of defense, and enable executive certification. Impacted IDIs should:

1. Look for opportunities to integrate with broader initiatives;
2. Extend the control capabilities that were put in place for other regulatory initiatives (e.g. BASEL, CCAR, SOX, etc.);
3. Exploit existing Master Data Management and meta-data management technologies;
4. Leverage advanced analytics and rules-based toolsets; and
5. Integrate enhanced processes with recovery and resolution planning requirements (i.e. living wills).

CIs have an opportunity to look beyond the regulatory requirements associated with the Rule to build a return on investment resulting from an enhanced view of the total customer relationship. Enhancing data capabilities that can support deeper insights to customer behavior and product holdings can be potentially leveraged for marketing and sales opportunities, increase share of wallet and support greater customer penetration.

KPMG

About the authors

KPMG has extensive knowledge of the requirements associated with the Rule, and a deep understanding of the activities required from CIs impacted by the new requirements.

KPMG has developed an assessment model and business requirements associated with the Rule and is actively engaged in assisting CIs with current state assessments, implementation planning, and remediation assistance.

KPMG's financial services professionals have a great depth of experience assisting banks and other financial institutions in understanding and preparing for complex regulatory requirements, including data and technology enhancement opportunities considering the requirements of Part 370.

Contact us

Ken Albertazzi
Partner, Advisory
Operations and Compliance Risk
T: 617-988-1061
E: kalbertazzi@kpmg.com

Benjamin Roberts
Partner, Advisory
Financial Services Solutions
T: 860-522-3200
E: broberts@kpmg.com

Nilesh Panchal
Principal, Advisory
Digital Enablement
T: 404-222-3000
E: nileshpanchal@kpmg.com

William Canellis
Director, Advisory
Operation and Compliance Risk
T: 973-912-4817
E: wcanellis@kpmg.com

Charith Mendis
Director, Advisory
Financial Services Solutions
T: 212-872-3571
E: cmendis@kpmg.com

Dane Roberts
Manager, Advisory
Financial Services Solutions
T: 212-954-6943
E: daneroberts@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia