IRON MOUNTAIN®

FDIC RECORDKEEPING REQUIREMENT DRIVING INFORMATION GOVERNANCE

The FDIC has issued rule 12 CFR Part 370: Recordkeeping for Timely Deposit Insurance Determination, requiring banks to establish two capabilities:

1. *configure its information technology system to be capable of calculating the insured and uninsured amount in each deposit account*
2. *maintain complete and accurate information needed by the FDIC to determine deposit insurance coverage with respect to each deposit account*

Regulators have become increasingly granular in their information management requirements on institutions (e.g. with regard to privacy, cybersecurity) – now specifying steps that must be taken in order to comply with a rule with an inarguable purpose – providing guaranteed insurance on bank deposits. Enhanced information governing regulations have come with a tremendous increase in penalties for non-compliance, not to mention the risk of reputational damage which goes well beyond the financial consequences.

On top of these already existing requirements, new ones continue to crop up and challenge the financial services industry.

A newly issued FDIC rule, **FDIC Rule 12 CFR Part 370**, requires sound information governance practices and is another rule driving activities including records retention, classification and automating records governance in banks.

This new rule requires financial institutions to have customer deposit account systems for traditional deposits as well as for more complex or pass-through accounts in order to capture data to calculate account holdings and insurance coverage. The more complex accounts may present challenges quantifying deposits or even identifying account ownership. Data must be accurate and include regular reporting. Banks are subject to audits and the FDIC will levy fines for regulatory violations.

Information governance (IG) is the overarching strategy for addressing new and existing regulatory requirements efficiently and effectively. Addressing these rules on a one-off basis is inefficient, costly and unsustainable.

WHAT YOU NEED TO KNOW ABOUT FDIC RULE 370

As with recent privacy regulations, FDIC Rule 370 gives banks ample time to address the new rule and implement the very specific requirements. These requirements are important because history shows that banks can and will fail. Furthermore, to avoid broader damage to the financial industry, the FDIC provides insurance to give banks and consumers a bit of a safety net. Therefore the FDIC must understand what funds are required to insure a bank's deposits.

THE KEY TO ADDRESSING THE MANY REGULATORY REQUIREMENTS AND AVOIDING NEGATIVE ACTIONS IS A SOUND INFORMATION GOVERNANCE PROGRAM.

Here's what banks need to know about FDIC Rule 370:

- The compliance deadline is April 2020. Therefore, action is required now.
- Financial institutions are intertwined. The actions of one, particularly a significant action such as a bank failure or major ruling, impacts others.
- Perhaps most important is ensuring there is confidence in the U.S. financial system including with insurance. Therefore:
  - Companies are to have systems and data to calculate account holdings and insurance coverage.
  - The rule requires accurate data and regular reporting.
  - Banks will be subject to audits on this rule.
  - The FDIC could levy fines for violations.

Recently, some regulatory reporting requirements have been reduced through regulators' burden reduction efforts, regulatory relief legislation, and tailoring of data requirements. These reductions, however, don't change regulators' expectations for managing data. In fact, some of the reductions in reporting have been offset by new data requirements, particularly for large complex firms. Furthermore, there's a general trend toward requiring more granular, product-level data and demanding it be more readily available. This trend underscores the need for strong enterprise data management practices and accountability.

WHY INFORMATION GOVERNANCE IS KEY TO FDIC RULE 370 COMPLIANCE

The key to addressing the many regulatory requirements and avoiding negative actions is a sound information governance (IG) program. Partnering with cross-functional areas and departments within your organization is critical to a successful program. These areas and departments include the line of business, risk, compliance, legal, IT and others.

A successful IG program manages information throughout its lifecycle with strong governance rooted in policy. In order to have strong information lifecycle management (ILM) in place you need to understand who owns what information, the information location, and the information classification from creation to disposition. Without this it's just not possible to ensure compliance, especially at scale, and effectively protect valuable, sensitive information.

Knowing and understanding what information you have, assessing any associated risks, identifying controls, and managing that information

throughout its lifecycle – according to policy – will help your organization maintain compliance and mitigate exposure to risk. To achieve this you need to:

- establish policy and procedures to manage information, including retention
- develop strategies and tools to manage data inventories and data maps
- create a framework to assess risks and prioritize data remediation activities
- find solutions for managing records such as discovery and classification

WHAT SPECIFIC ACTIONS SHOULD YOU CONSIDER TO ADDRESS FDIC RULE 370 NOW?

High-value IG activities should be part of an enterprise information governance (EIG) program that provides a roadmap for sustainability and continuous improvement. Existing IG programs may be augmented and nascent programs can begin with priority issues. Targeted activities should include the following, starting with the foundational elements:

- ensure policies and rules are documented, published and applied
- identify data sources
- digitize hard copy
- implement data mapping – as many are doing with data privacy
- deploy content classification
- utilize analytics
- provide education and awareness for employees
- ensure quality assurance and auditing

In summary, data quality and availability are greatly impacted by IG and lifecycle management. Classification at creation, linkage with regulatory citations and disposition enable lifecycle management. It also mitigates the tremendous challenges of velocity, veracity, variety and volume. Information governance enhances quality and availability of information by identifying systems of record and reducing the noise of dated, inaccurate and unneeded data.

This, in turn, will help banks not only meet the requirements of the new FDIC Rule 370 but ensure continued compliance with other existing and future rules and regulations.