FDICIA readiness: What you need to know and next steps

Federal Deposit Insurance Corporation Improvement Act of 1991

The Federal Deposit Insurance Corporation (FDIC) passed the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) in an effort to strengthen the banking environment and to reduce the negative impacts of the savings and loan crisis of the 1980s and early 1990s.The Act included a number of key provisions affecting the banking industry, including primarily:

- **Prompt corrective action (PCA) provision**. The PCA provision requires federal banking agencies to take action when an insured depository institution's capital is classified as undercapitalized, significantly undercapitalized or critically undercapitalized (as determined by selected capital measures). In an effort to minimize losses for all involved parties, these interventions depend on the level of undercapitalizationundercapitalization and may include being placed into conservatorship or receivership.
- **Least-cost resolution provisions**. The least-cost resolution provisions require the FDIC to choose a resolution method for failed insured depository institutions that minimizes the costs to taxpayers. The FDIC is limited in its ability to absorb losses with an exception for preserving institutions that are too big to fail.
- **Improved examinations**. FDICIA adjusted the conditions that allowed an institution to qualify for an 18-month, full scope, on-site examination, in effect increasing the volume of institutions subject to these examinations. FDICIA also required the appropriate Federal banking agencies to improve the quality of their examinations through reviews of the agencies and their staff training and increasing the number of examiners, supervisors and others employed by the agencies.
- **Truth in Savings Act (TISA)**. TISA was enacted as part of the passage of FDICIA and requires banks to disclose to consumers the rates (annual percentage yields) and fees associated with their accounts.

Section 36 and Part 363

Section 36 of the Federal Deposit Insurance Act (which was added by section 112 of FDICIA) and Part 363 of the FDIC's regulations aim to facilitate the early identification of problems in financial management at insured depository institutions over a certain asset threshold size. The institutions subject to the requirements under section 36 and Part 363, commonly referred to as *covered institutions*, are currently defined as those institutions with $500 million or more in total assets. Additional requirements become effective once a covered institution reaches $1 billion in total assets.

Annual audits and reporting package submissions

Overview and reporting deadlines

The Part 363 annual reporting package should include a combination of items, including financial statements, audit reports and management reports, with the specific requirements being dependent on the size of the covered institution.

Reporting packages are due within 90 days after the end of the covered institution's fiscal year if it is (a) a public company or (b) a subsidiary of a public holding company and its consolidated total assets comprise 75% or more of the consolidated total assets of the public holding company as of the beginning of its fiscal year.

Reporting packages are due within 120 days after the end of the covered institution's fiscal year if it is (a) not a public company or a subsidiary of a public company or (b) a subsidiary of a public holding company and its consolidated total assets comprise less than 75% of the consolidated total assets of the public holding company as of the beginning of its fiscal year.

Audited financial statements

Audited, comparative financial statements and a corresponding independent public accountant's report on the audited financial statements are required for all covered institutions. The level of financial statements that satisfy the reporting requirements depends on the organizational structure of the consolidated company and the relative size of the insured depository institution (IDI). For IDIs that are subsidiaries of holding companies, the audited financial statements submitted may be the consolidated financial statements of the top-tier or any mid-tier holding company if the total assets of the IDI (or multiple IDIs if applicable) comprise 75% or more of the consolidated total assets as of the beginning of the fiscal year.

All other requirements in the reporting package may also be satisfied at the holding company level if:

- The services and functions of the IDI and the holding company are similar.
- The IDI has, as of the beginning of its fiscal year, total assets less than $5 billion or total assets greater than $5 billion and a composite CAMELS rating of 1 or 2.

Scenario 1: Bank A is the wholly owned subsidiary of Holding Company A. Per its December 31, 20X1, Call Report, Bank A has $3.5 billion in total assets. The consolidated entity has $3.8 billion in total consolidated assets as of December 31, 20X1. Considering that Bank A comprises 92% of the total consolidated assets, the services and functions are comparable in nature for both entities and the IDI (Bank A) has less than $5 billion in total assets, the Bank A may satisfy its reporting requirements with consolidated statements and reports for its 20X2 reporting period.

Scenario 2: Bank M is the wholly owned subsidiary of Holding Company M. Per its December 31, 20X1, Call Report, Bank M has $10 billion in total assets. The consolidated entity has $13 billion in total consolidated assets as of December 31, 20X1. Bank M's most recent FDIC examination as of September 30, 20X1, resulted in a composite CAMELS rating of a 2. Considering that Bank M comprises 76% of the total consolidated assets, the services and functions are comparable in nature for both entities, and the IDI (Bank M) has over $5 billion in total assets and a composite CAMELS rating of a 2, Bank M may satisfy its reporting requirements with consolidated statements and reports for its 20X2 reporting period.

Scenario 3: Bank Z is the wholly owned subsidiary of Holding Company Z. Per its December 31, 20X1 ,Call Report,Bank Z has $10 billion in total assets. The consolidated entity has $13 billion in total consolidated assets as of December 31, 20X1. Bank Z's most recent FDIC examination as of September 30, 20X1, resulted in a composite CAMELS rating of a 3. Considering that Bank Z comprises 76% of the total consolidated assets, the IDI (Bank Z) may satisfy its annual audited financial statement requirement with its consolidated financial statements. However, because Bank Z received a composite CAMELS rating of a 3, the bank cannot satisfy its other reporting requirements with consolidated reports. Thus, it is likely that Bank Z will submit its reporting package for 20X2 with audited financial statements and reports for Bank Z only. If the use of consolidated financial statements reporting is preferred (with other reporting requirements at the IDI level), the audit should be performed at a level such that bank only financial statements could have been presented as contemplated by AU-C 940, Exhibit D.3. Specifically, the auditor would be required to perform procedures necessary to obtain sufficient appropriate audit evidence to enable the auditor to express an opinion on the IDI's financial statements and on its ICFR.

Management report

Management is required to provide a report regarding its responsibilities and certain conclusions with respect to internal controls and compliance with designated laws and regulations.

The following elements of the management report are required based on the size of the coverered institution:

	Total assets	
	At least $500 million but less than $1 billion	$1 billion or more
Management report that includes:		
Statement of responsibilities for preparing financial statements, establishing and maintaining an adequate internal control structure and complying with designated laws and regulations	■	■
Assessment of and conclusion relating to compliance with designated laws and regulations pertaining to insider loans and dividend restrictions	■	■
Assessment of effectiveness of internal control over financial reporting (ICFR) as of the fiscal year-end		■

Independent auditor's report on ICFR

In certain cases, an assessment of the effectiveness of ICFR is also required as part of the annual reporting package submitted to the FDIC. An effective internal control structure is considered to be critical to the safety and soundness of insured depository institutions.

An independent auditor's report on ICFR is required when a covered institution has $1 billion or more in total assets. No such assessment and report by an independent auditor is required when total assets are under $1 billion.

For institutions that are not public filers, the internal controls audit is conducted in accordance with the American Institute of Certified Public Accountants' (AICPA) standards (AU-C 940, An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements). For institutions that are public filers and subject to a Sarbanes-Oxley Act (SOX) 404 integrated audit, the internal controls audit is generally conducted in accordance with the Public Company Accounting Oversight Board's (PCAOB) standards (*AS 2201, An Audit of Internal Control Over Financial Reporting That Is Integrated With An Audit of Financial Statements*). For institutions that are public filers, but that are not subject to a SOX 404 integrated audit, the internal control audit is generally conducted in accordance with AICPA standards (AU-C 940).

Audit committee

Part 363 requires each covered institution to establish an independent audit committee of its board of directors that is comprised of outside directors. Outside directors are defined as individuals who are not, and within the preceding year have not been, an officer or employee of the institution or any of its affiliates.

Ultimately, the audit committee is responsible for the appointment, compensation and oversight of the independent public accountants and reviewing the reports included in the annual report submitted to the FDIC.

For covered institutions with total assets of $500 million but less than $1 billion, the majority of the audit committee's members (outside directors) should be independent of management.

For covered institutions with total assets of $1 billion or more, all audit committee members should be outside directors who are independent of management. At least annually, the board of directors should determine whether the existing and potential audit committee members are independent of management.

When the covered institution has total assets over $3 billion as of the beginning of its fiscal year, the audit committee should further include members with banking or related financial management expertise, should have access to its own outside counsel and should not include any large customers.

In order to determine whether existing or prospective audit committee members are independent of management, consideration should be given not only to the member itself but also to any relationships or affiliations that the member may have with related parties of the institution. Paragraph 28 of Appendix A to Part 363 (*Guidelines and Interpretations*) includes guidance for this determination.

FDICIA readiness

Preparation is critical to success in FDICIA compliance. An institution should consistently monitor its growth and strategic plan in an effort to project when it is approximately one to two years from reaching the $500 million and $1 billion thresholds. This will allow the organization to ensure compliance once the asset threshold is triggered, to identify necessary resources and to develop a thorough plan that integrates management, the audit committee, the board of directors, the independent public accountant and internal audit. The best advice may be to begin acting like an FDICIA-covered institution before the provisions are effective.

In order to ensure your organization is ready to implement the requirements of FDICIA, consider the following:

Measure total assets

The provisions of FDICIA are effective when total assets meet or exceed $500 million as of the beginning of the fiscal year. Total assets over $1 billion trigger additional requirements under Part 363.

When measuring total assets, the institution should use total assets as reported on its most recent Report of Condition (Call Report). The date of the most recent Call Report should coincide with the end of the preceding fiscal year for those institutions with a fiscal year-end that ends on a calendar quarter (e.g., March 31, June 30, September 30, December 31). In other words, to evaluate applicability for the 20X2 fiscal year, a calendar year-end institution would use the Call Report from December 31, 20X1, which also represents the opening balance as of January 1, 20X2. If the institution's fiscal year-end falls on a date other than the end of a calendar quarter, it should use the Call Report for the quarter-end immediately preceding the end of its fiscal year (e.g., March 31 for an April 30, noncalendar quarter fiscal year-end).

December 31, 20X0:

Total assets as of December 31, 20X0: $477 million

December 31, 20X1

Total assets throughout fiscal year:

- March 30: $480 million
- June 30: $501 million
- September 30: $499 million
- December 31: $502 million

FDICIA does not apply for 20X1, as total consolidated assets for December 31, 20X0 were not over $500 million.

December 31, 20X2

Total assets throughout fiscal year:

- March 30: $505 million
- June 30: $510 million
- September 30: $511 million
- December 31: $520 million

FDICIA applies for 20X2 as total consolidated assets for December 31, 20X1, were over $500 million.

The measurement exercise in the preceding graphic is a continuous process. If a covered institution's total assets fall below the applicable threshold in a subsequent period, the covered institution remains subject to FDICIA requirements until its next measurement period (i.e., the next fiscal year-end Call Report date). Modifying and expanding upon the previous example, if the covered institution's total assets had fallen below $500 million as of March 31, 20X2, and remained under $500 million in total assets as of December 31, 20X2, then it would not be subject to requirements for the 20X3 audit. However, it would still be subject to requirements for 20X2 because the threshold was met as of December 31, 20X1.

This example would also apply when a covered institution is approaching the $1 billion threshold, which would trigger the additional requirements under Part 363.

Create a FDICIA road map and detailed project plan

Once the institution determines it is approaching or has already met the asset thresholds for FDICIA, management should work to create a detailed FDICIA road map and project plan. Starting with the end date in mind (e.g., the first annual audit for which the FDICIA reporting package must be submitted or the first period in which an ICFR audit is required), the institution should work backward to determine key milestones. From this road map, we should then create a detailed project plan that incorporates various stakeholders, including management, operational leaders, the audit committee, the board of directors and the internal audit function—that address all of the elements of compliance.

For the internal audit function specifically, a one-to-two year plan to perform additional risk assessment, identify key controls for FDICIA purposes, ensure compliance with the Committee of Sponsoring Organization's (COSO) 2013 frameworks (or other acceptable framework) and either develop a testing plan or integrate existing testing with the FDICIA requirements is integral to FDICIA readiness.

The covered institution should consider a dry run year or two for the internal controls evaluation to allow time to confirm and update controls (as needed), identify and remediate any existing control deficiencies and properly train personnel. It may be helpful to start with less complex areas, such as cash and deposits, then move on to higher-risk sections such as the allowance for loan losses.

Auditor independence and review of nonaudit services

The independent public accountant must comply with the independence standards of the AICPA, the Securities and Exchange Commission (SEC) and the PCAOB for all covered institutions, regardless of whether the covered institution is a public company.

SEC and PCAOB standards are generally more restrictive than AICPA standards with respect to permissible nonaudit services. Thus, as a covered institution nears the $500 million total asset threshold, it is important to inventory the services performed by the independent public accountant and to determine whether those services remain permissible under the SEC and PCAOB independence standards.

Common nonaudit services that are permissible under AICPA standards, but not under SEC and PCAOB standards include, but are not limited to:

- Preparation of financial statements, including rolling forward report templates, preparation of or substantial assistance with the statements and footnotes; and report processing functions such as typing, printing, copying and binding.
- Appraisal or valuation services or fairness opinions.
- Internal audit services, including outsourced loan review.
- Tax services relating to marketing, planning or opining in favor of the tax treatment of a transaction that is a confidential transaction under U.S. Treasury regulations or that is based on an aggressive interpretation of applicable tax laws and regulations (Tax compliance services generally present little or no threat to auditor independence and are permissible).
- Tax services to a person in a financial reporting oversight role or an immediate family member (i.e. spouse, spousal equivalent or dependent).

Once a covered institution meets $500 million in total assets, any permitted nonaudit services should be discussed with and pre-approved by the audit committee prior to commencing such services under SEC independence rules. Refer to Rule 2-01 of Regulation S-X and PCAOB Rules 3524-3526 for further details relating to the audit committee's role in the approval of permitted nonaudit services.

Gain an understanding of COSO 2013

COSO released an updated version of its *Internal Control – Integrated Framework* in 2013 that supersedes the 1992 framework. This updated framework retains the five components of internal control (control environment, risk assessment, control activities, information and communication, and monitoring) and adds 17 internal control principles and 81 points of focus considered necessary for an effective internal control environment. While other frameworks may be acceptable, COSO 2013 is the most prevalent.

Evaluate and educate the audit committee

As the institution approaches the applicable asset thresholds, it should also consider the existing makeup of the board of directors and, if applicable, its audit committee. Once an institution reaches $500 million in total assets, it is required to have an independent audit committee. Considering one of the primary responsibilities of the audit committee is to appoint an independent public accountant, the institution should ensure it has an appropriate audit committee in place prior to reaching this threshold and before engaging the independent public accountant for its initial FDICIA audit.

The audit committee should also be educated in the independence rules and knowledgeable of the nonaudit services, if any, performed by the independent public accountant. Any required preapprovals of nonaudit services should be scheduled and completed.

Refer to RSM's Audit Committee Guide for Financial Institutions for further information on the audit committee's responsibilities, including its role in evaluating the control environment and risk assessment, as well as specific FDICIA-related considerations.

Discuss oversight responsibilities with the board of directors

Beyond discussing the basic provisions and requirements of FDICIA, the board of directors should also understand its responsibilities for oversight. Specifically, Part 363 requires that the board of directors determine whether each existing or potential audit committee member meets the requirements of being an outside director and, as applicable based on the asset threshold of the covered institution, is independent of management. The minutes of the board of directors' meetings should contain the procedures performed, basis for determinations and results of these assessments.

The board of directors should also consider the management team's experience and expertise to determine if the most appropriate people are in place once the FDICIA requirements apply. Management needs to have the ability to make the assessments included in management's report, including a deep understanding of the entity and its control environment and sufficient oversight over the operations of the institution. Additional members of management may be needed to supplement the knowledge and experience of existing members of management, particularly with respect to internal controls and risk assessment.

Assessment and (or) implementation of an internal audit function

With the requirement that management establish and maintain an adequate internal control structure, there is generally a need for a formal, sophisticated internal audit function at the institution. Depending on the current state of the internal audit function, it may be necessary to supplement personnel, restructure reporting lines and enhance procedures performed throughout the year. Generally, the organization should have established processes for tasks such as risk assessment, personnel education, evaluation of control design, testing of operating effectiveness, reporting of results and monitoring. Additionally, these processes should be performed and overseen by competent individuals with requisite experience. Whether the internal audit work is to be performed internally or externally, the responsibility still rests with management for implementing and monitoring a sound control environment at both the entity and transaction levels.

Remember the information technology (IT) function

In order to conclude on the effectiveness of internal controls as a whole for the covered institution, consideration must be given to the IT environment and related controls. A formal internal audit plan may need to be developed, or an existing plan may need to be expanded to meet FDICIA requirements.

For the entity as a whole and each in-scope IT application identified, the institution should evaluate logical security, security administration, operations, change management, business continuity or disaster recovery, cybersecurity and vendor management.

Remediate any identified material weaknesses in ICFR

A material weakness is defined as a deficiency, or a combination of deficiencies, in internal control over financial reporting, that results in a reasonable possibility that a material misstatement of the financial statements will not be prevented or detected and corrected in a timely manner.

Pursuant to Part 363, management and the independent public accountant are precluded from concluding that ICFR is effective if one or more material weaknesses exist. Thus, the institution should work to correct any known material weaknesses in ICFR and develop safeguards in the control environment to reduce the risk that material weaknesses arise.

Consider the need for entity-wide training

Often those responsible for executing many of the controls on a regular basis (commonly referred to as control operators) may not understand the implications of these procedures from a regulatory standpoint. In order to support a sound internal control environment, there should be an appropriate level of awareness and commitment from various levels within the organization. It may be beneficial to host training sessions for employees throughout the organization to educate them on topics such as the COSO framework, FDICIA, the internal and external audit processes and the importance of their role as control operators in ensuring that controls are properly designed and operating effectively and that adequate documentation of their procedures is in place.

How can RSM help?

RSM has assisted a number of banks in sorting through the complexities of FDICIA compliance, including helping institutions as they cross over the $500 million and $1 billion total asset thresholds. For banks who are not audit clients, we can provide assistance in initial FDICIA compliance efforts or help in optimizing the existing internal control environment and compliance program. We can also provide certain outsourcing, co-sourcing (partnering) or loaned staff services. For banks who are audit clients, we can provide limited assistance in the assessment of enterprise risk management activities and certain regulatory compliance matters.

Our firm's size and volume of work enable us to provide you with industry specialists rather than generalists. You will not have to train our professionals on your business model. RSM clients value the depth and breadth of our professionals' experience—experience gained as bank executives, banking regulators, internal auditors, IT specialists and accounting professionals.

Over the years, we have developed a solid reputation as trusted advisors and thought leaders in the banking industry by consistently delivering proven professionals who understand your operating environment and offer timely and constructive solutions to your most pressing business needs.

Prepared by:

- Amber Sarb, Senior Manager, National Professional Standards Group, RSM US LLP
  amber.sarb@rsmus.com, +1 847 413 6453

- Mike Lundberg, Partner, National Professional Standards Group, RSM US LLP
  mike.lundberg@rsmus.com, +1 612 455 9488

February 2024

2108548