

FINANCIAL SERVICES BOARD INSIGHTS

FDICIA Requirements
Updated for Small and
Mid-Sized Banks

AI, Cybersecurity,
and Audit Committee
Oversight

Shifts in OCC Regulatory
Oversight Tailored to Bank
Size and Risk Profile

Compliance and Internal Audit:
A Dynamic Partnership for
Strong Governance

FDICIA Requirements Updated for Small and Mid-Sized Banks

For more than three decades, the Federal Deposit Insurance Corporation Improvement Act (FDICIA) – which includes 12 CFR Part 363, the regulation that dictates how large insured depository institutions must comply with audit and reporting mandates – has been in place to address the savings and loan crisis of the 1980s. The FDIC recently **updated parts of the Act with** many of these changes **benefiting** smaller institutions.

New FDICIA Requirements for 2026

On Nov. 25, 2025, the FDIC adopted amendments to FDICIA, raising total asset thresholds for board audit committee composition, independent audits, and other reporting obligations, thereby reducing compliance burdens for smaller and mid-size institutions. Effective Jan. 1, 2026, the new total asset thresholds and corresponding requirements are as follows:

For institutions with \$1 billion to \$5 billion in total assets:

- All audit committee members must be outside directors, a majority of which must be independent of management.
- Mandatory independent external audit of financial statements.
- Management must attest to the effectiveness of internal controls including those critical to the bank's operations and risk profile, IT systems, and fraud prevention.

For institutions with over \$5 billion in total assets:

- Mandatory Internal Control over Financial Reporting (ICFR) assessments and external auditor attestation.
- All audit committee members must be independent outside directors.
- Audit committees must include members with banking or related financial management expertise, have access to outside counsel, and not include any of the institution's large customers.

Which Institutions do the FDICIA Changes Impact?

Although the recent FDICIA changes removed nearly 800 institutions from the general scope of applicability for Part 363, the regulation continues to cover financial institutions holding approximately 95 percent of industry assets. Banks with total assets that fluctuate around the \$1 billion and \$5 billion thresholds must closely monitor their total assets to plan to meet the different requirements.

The changes to Part 363 also allow for future adjustments to the new thresholds based on inflation. The limits will be reviewed and potentially updated every two years or, if inflation exceeds 8 percent in a single year, sooner. The first planned update is anticipated to be effective October 2027.

Benefits of FDICIA Updates

Since these updates address outdated fixed-dollar thresholds that subjected smaller banks to requirements meant for larger ones, smaller institutions should experience an easing of financial reporting burdens that may free up resources and funding for other uses, such as investments in innovation, customer experience technology, and fraud prevention.

The updates also represent an opportunity to fully reassess overall risk profiles, internal controls, and compliance efforts.

Moreover, even though the FDICIA updates have removed the requirement for independent external financial statement audits for banks with under \$1 billion in assets, audit committees may choose to continue these audits for strategic planning purposes and growth projections, as well as to inform decisions about potential acquisitions.

Finally, audit committees may find it easier to recruit members because the compensation threshold that determines whether a director is independent of management increased from \$100,000 to \$120,000.

Our team members are experts at interpreting these and other compliance and regulatory changes and assisting financial institutions in evaluating and adjusting internal controls and compliance efforts for effective governance that supports long-term growth objectives. For personalized guidance and recommendations specific to your financial institution, contact Kevin Frank, CPA, at kevin.frank@rehmann.com or 989.799.9580, or Alicia Prichard, CPA, at alicia.prichard@rehmann.com or 734.302.4142.



AI, Cybersecurity, and Audit Committee Oversight

It's important for audit committee members, in their oversight role to understand how Artificial Intelligence (AI) impacts their institution's day-to-day operations. For example, AI could be used in financial reporting, enterprise-wide risk management, fraud risk mitigation, and data privacy and security.

To ensure their effectiveness, adaptive AI models rely on data quality, accuracy, reliability, and integrity. As such, audit committees should focus on and understand data management related to the following:

- **Data governance** to ensure data privacy and access controls are established and implemented with supportive employee education and training.
- **Data security** to ensure sensitive or confidential information fed into AI models is protected, especially if the data leaves financial institutions' secure IT systems.
- **Transparency** to help regulators understand how the selected AI models operate, respond, and provide conclusions and reporting that informs decisions about policies, operations, and strategic planning.
- **Human oversight** procedures to ensure people review, evaluate, and are accountable for AI outcomes to avoid overreliance and reduce risk.

Cybersecurity First

Because the use of AI integrates systems and data, which is often shared outside financial institutions' networks, it can increase the risk of cyberattacks. Ongoing investment in thorough monitoring and oversight of cybersecurity measures is critical to protect

confidential data and marketplace reputation. Aligning processes to recognized frameworks like those recommended by the National Institute of Standards and Technology (NIST), International Standard for Organization (ISO), or Cybersecurity and Infrastructure Security Agency Industrial Control Systems (CISA ICS) provides an oversight structure to track effective, secure, and compliant AI use and data collection.

How AI Can Address OBBB Reporting Requirements

The One Big Beautiful Bill Act of 2025 (OBBB) includes new reporting requirements with tax benefits for banks, credit unions, and their borrowers. AI solutions can help ensure accurate and secure collection and reporting of data not only to comply with OBBB requirements, but also to realize financial benefits, such as:

Agricultural Loans: Qualified lenders can deduct up to 25 percent of interest income received for loans originated after Jul. 4, 2025. The loans must be secured by real property that is located in the U.S. or a U.S. territory and produces agricultural products, supports a fishing or seafood processing businesses, or operates an aquaculture facility. When accurately tracked and accounted for, this new deduction provides financial incentive to grow this segment of the loan portfolio in certain regions.

Auto Loans: For tax years 2025 through 2028, individual taxpayers who purchase qualifying new vehicles for personal use are entitled to an annual deduction of up to \$10,000 of interest paid on loans originated after Dec. 31, 2024.

On Dec. 31, 2025, the IRS proposed regulations to clarify lenders' auto loan reporting requirements, including: Lenders

receiving \$600 or more in interest on a qualifying auto loan would be required to report.

- Lenders required to report must provide to the IRS and taxpayers: the name, address, and taxpayer identification number of the payor of record and the interest recipient; the amount of interest received for the calendar year; the outstanding loan principal as of the beginning of the calendar year; date of loan origination; year, make, model, and VIN of the vehicle that secures the loan; and date the vehicle was acquired.

What Audit Committees Need to Know About Their Institution's Use of AI

Realizing the full potential of AI means audit committees must fully understand the risks and opportunities the tool poses to ensure management has defined and implemented policies, processes, and controls that govern the acceptable use of AI. Audit committee members should ask management questions about AI responsible use and cybersecurity protections, such as:

- How are you using AI? What are your competitors doing, and how are you maximizing opportunities?
- What are your procedures to test AI models for accuracy, reliability, data bias, and other risks? How is human review verifying these outcomes and for ongoing monitoring of AI post-implementation?
- Are you using AI models you consider to be higher risk? Why and what are the benefits?
- How is data used, protected, and secured against risks of cybercrime and data breaches?
- How are employees educated and trained on the importance of cybersecurity practices? How are you documenting that leadership provides clear guidance to employees about their responsible use of AI to support data security?
- What's your business continuity plan for a data breach resulting from a cyberattack or AI failure?

By prioritizing cybersecurity and leveraging proven principles regarding the acceptable use of AI, your financial institution can not only strengthen its data management and reporting but also upgrade digital defenses with strategies that protect systems, drive innovation, deliver on customer expectations, and reduce unnecessary risk. Contact your Rehmann advisor or Liz Ziesmer, CPA, at liz.ziesmer@rehmann.com or 616.975.4100 or Jessica Dore, CISA, at jessica.dore@rehmann.com or 989.799.9580 for a personal consultation.

Shifts in OCC Regulatory Oversight Tailored to Bank Size and Risk Profile

Recent Office of the Comptroller of the Currency (OCC) announcements support community banks by reducing regulatory burdens, reflecting the agency's efforts to align its supervisory frameworks with the size and risk profile of an institution.

In an announcement regarding the changes, Comptroller of the Currency Jonathan V. Gould noted, "Community banks provide the majority of small business lending and are essential to a diverse, competitive and resilient financial system. Today's actions further relieve community banks of unnecessary regulatory requirements and seek to better position them to help fuel job creation and economic development in local communities across the country."

BSA/AML Begins Feb. 1, 2026: What Community Banks Need to Know

The new Community Bank Minimum Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Procedures, announced Nov. 24, 2025, and effective Feb. 1, 2026, reduce burdens on community banks by emphasizing examiner discretion to:

- Rely on satisfactory independent testing to form a basis for conclusions for specific examination procedures.
- Carry forward prior examination conclusions for the training and BSA Compliance Officer pillars for one examination cycle when there have not been significant changes to the bank's risk profile and in consideration of other relevant factors.

- Determine whether and to what extent to perform transaction testing, or if it's appropriate to limit testing to analytical or other reviews.

New BSA/AML: What to Expect from Examiners

The new Community Bank Minimum Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Procedures focus examiners on three primary objectives:

• Scoping and Planning

Examiners will develop an understanding of the bank's money laundering/terrorist financing (ML/TF) and other illicit financial activity risk profile, develop a risk-focused examination scope, and document the BSA/AML examination plan.

• BSA/AML Compliance

Examiners will determine whether the bank has designed, implemented, and maintains an adequate BSA/AML compliance program that meets BSA regulatory requirements.

• Develop Conclusions and Finalize the Examination

Using the bank's risk profile and overall compliance with BSA regulatory requirements, examiners will determine the adequacy of the bank's BSA/AML compliance program, and document and communicate examination findings to the bank.

MLR Revisions: No More Annual Mandatory Data Required, Input Requested

The OCC also announced that as of Nov. 24, 2025, it has discontinued annual mandatory data collection from community banks under the Money Laundering Risk (MLR) System.

It also issued a request for information (RFI) to help the OCC better understand the

challenges community banks face with core service providers and other essential third-party service providers in areas like contract negotiations and terms, billing practices, oversight, due diligence, core and legacy system conversions, and data access.

The RFI includes questions regarding potential OCC actions that could address these challenges, such as reduced burdens related to supervisory practices, policies, and guidance. The comment period closed in January 2026, and the Rehmann team continues to monitor outcomes of the OCC final report.

Changes to CBLR Framework Proposed

Finally, the OCC noted that its ongoing work includes a proposal to reduce the community bank leverage ratio (CBLR) requirements. The comment period for the proposed amendments ends Jan. 30, 2026; further details, including potential implementation timelines, are expected to come in early to mid-2026.

Your Takeaway

Regulatory and compliance burdens are rapidly evolving, with many changes that stand to benefit smaller and mid-sized community banks. Bank boards should invest the time now to understand current, pending, and proposed updates that could significantly impact their organization's strategic planning, growth, compliance, and merger & acquisition decisions.

To help your board or organization navigate these and other changes, contact your Rehmann advisor or Beth Behrend, CCBCO, CBAP, at beth.behrend@rehmann.com or 616.975.4100 or Mynesha Phifer, CCBCO, at mynesha.phifer@rehmann.com or 734.302.4152.



Compliance and Internal Audit: A Dynamic Partnership for Strong Governance

Compliance and internal audit are two closely related but distinct functions that work collaboratively to support a financial institution's internal controls and risk management. To fulfil their oversight role, board members should be familiar with the two functions' roles and responsibilities and how they interact to support effective corporate governance.

For example, compliance professionals ask, "Are we following rules and controls, as well as meeting regulatory requirements?" whereas internal audit asks, "Are the rules and controls effective, and are we managing risks effectively?"

Here's a deeper look at the two functions' similarities and differences.

	Compliance	Internal Audit
Why	To monitor and manage adherence to external laws and regulations, and internal policies.	To provide objective evaluation of risk management, governance, and internal controls.
Scope	Compliance-related areas based on regulations that impact the institution.	Covers all areas of the institution including lending, information technology, operations, human resources, accounting, etc.
When	Day-to-day monitoring to implement and adjust policies to prevent violations.	Periodic audits based on risk assessment and annual audit plan.
How	Develops, communicates, and implements compliance programs and tools.	Systematic use of formal audit methodologies to test controls and processes.
What	Reports to department heads with critical issues escalated to senior leadership.	Reports to the audit committee identified deficiencies and proposed corrective actions, and verifies that management implements timely solutions.



Different Approaches with a Similar Goal

Compliance professionals monitor day-to-day processes, procedures, and documents to determine if regulatory requirements are being met. An effective compliance function identifies, sets, and adjusts policies and procedures, resulting in fewer findings during a formal audit or regulatory examination.

An independent internal audit function has no involvement in developing or executing programs but examines transactions and activity logs based on risk to determine effectiveness and/or accuracy of financial and non-financial processes and internal controls. Examinations may include business continuity plans, compliance programs, credit practices, IT and cybersecurity, financial reporting, and third-party risk management activities.

Internal audit and compliance should work together by collaborating closely to create a unified approach to risk management. When these two functions coordinate their efforts, they streamline processes, minimize redundant activities, and prevent organizational silos that could hinder effective data collection and risk tracking. This partnership helps optimize resources, ensuring strong corporate governance, robust ethical standards, effective internal controls, and enhanced fraud prevention. Their joint efforts support a comprehensive compliance and risk oversight framework, making it easier to identify and address potential issues proactively.

Your Takeaway

The board plays a crucial role in risk management by providing oversight and strategic direction to ensure that risks are properly identified, assessed, and mitigated. Board members are responsible for setting the organization's risk appetite, reviewing risk management policies, and monitoring the effectiveness of internal controls and compliance programs. They collaborate closely with audit and compliance professionals, ensuring that critical issues are escalated and addressed by management, and that corrective actions are implemented in a timely manner.

To learn more about the dynamic relationship between compliance and internal audit, and to maximize your role as a knowledgeable and engaged board member, contact your Rehmann advisor or Kristy Clark, CPA, CIA, at Kristy.Clark@rehmann.com or 248.952.5000.

Rehmann is a financial services and business advisory firm. We excel at helping clients because we take a collaborative, personalized approach and build a customized team of specialists to help them achieve their objectives. We focus on the business of business — allowing people to focus on what makes them extraordinary. The firm started as a CPA firm more than 75 years ago. Now, we are a multifaceted advisory firm that helps businesses and high-net-worth families maximize potential. Clients who work with us want us to be more than a vendor. They want collaboration, innovation, and continuous improvement.