FALL 2026

FINANCIAL SERVICES BOARD INSIGHTS

What you need to know about Other Real Estate Owned (OREO)

While OREO is not a new concept for financial institutions, from 2020 to 2024, OREO foreclosure transactions were relatively infrequent. A recent rise in the number of distressed properties and quicker asset dispositions has led to consistent double-digit increases in year-over-year foreclosure auction activity.

As a result, it is important for financial institution leadership to revisit guidance on how to accurately categorize and report OREO assets' fair value, on-going valuation, and any income or loss resulting from a sale. If your institution has OREO on the books, this article is for you.

Accounting for transfer into OREO

OREO is generally considered to be acquired when the institution receives possession (physical possession or control) of foreclosed or repossessed property. In general terms, for residential real estate, the loan commonly should be classified as OREO once a Sherriff Sale is completed, even if there is a redemption period. Legal definitions of when possession or control is considered to transfer can also vary by state. The value of the property must be initially recorded at its fair value, less estimated costs to sell the property at the time it is moved into OREO. Any reductions in the loan balance at transfer are recorded as a charge-off to the allowance for credit losses (ACL). This adjusted "fair value" amount becomes the asset's new cost basis. If the fair value of the assets exceeds the loan balance, a gain could be recognized. Therefore, it is prudent to challenge the assumptions used in determining the fair value to ensure that a gain truly does exist.

Accounting for the sale of OREO

Developed by the Financial Accounting Standards Board (FASB), Accounting Standards Codification (ASC) Topic 606, Revenue from Contracts with Customers, was effective for non-public companies in 2019, providing clearer accounting guidance to evaluate and report foreclosed properties. However, as noted above, from 2020 to 2024, OREO foreclosure transactions were relatively infrequent, so many institutions did not need to regularly evaluate these transactions under ASC Topic 606.

When an OREO property is sold, the financial institution must evaluate the transaction under the five steps of ASC 606, to ensure the transaction meets the requirements to be considered a sale. It is important to evaluate the buyer's ability to pay the agreed upon sales price. If full consideration is received from the buyer and all security interest is transferred at the time of the sale, then revenue and any gain or loss can generally be recorded at the time of the sale. If the sale is internally financed and there is uncertainty about the buyer's ability to repay, then it is possible that the gain or loss will not be recorded at the time of the sale.

No two sales are the same, so it is important that each sale is evaluated individually under ASC 606.

The bottom line

- Accurate initial valuation of a foreclosed or repossessed property is critical to accurate accounting at the time the property is deemed to be acquired and subsequent reporting.
- An institution can recognize the entire gain or loss of an OREO sale only when control of the property fully transfers to the buyer, such as through a duly recorded title transfer.
- If an institution provides the buyer with financing but retains significant continuing involvement or does not pass full control of the OREO asset to the buyer, then the transaction may not qualify for "sale accounting" and payments are treated as a deposit liability until sale criteria are met.

Key Consideration of Board Oversight

As part of their overall oversight and discussions of OREO, directors may consider the following questions:

- Who is responsible for transactions in this area and does the accounting team have insight into the activity?
- What types of valuations are being obtained and frequency to ensure it is truly reflective of current market value?
- Are we seeing an increase in OREO because of isolated situations, or is it an early indicator of broader credit deterioration?
- Have our policies, people, systems, controls and third-party resources kept pace with the increase in OREO activity.

OREO accounting requirements can be complex. We can streamline valuations and advise your institution on the development and implementation of accurate accounting processes and controls. Contact Kevin Frank at Kevin.Frank@rehmann.com or 989-797-8346 for more information.

Fintech Partnerships — Key Considerations for Directors

Just two years ago, the financial services industry questioned whether fintech business models would be sustainable. Today, fintech revenue reports indicate that 74% of the largest 85 public fintechs are profitable, versus 68% in 2024, and fintech revenue is growing 22% year over year, four times faster than financial institutions revenue. The majority of fintech revenues are derived from payments processing and lending services.

As financial institutions continue to explore partnerships with fintech companies — to accelerate innovation, improve customer experiences, expand product offerings, and increase operational efficiency — regulators continue to emphasize caution.

While many activities may be outsourced to fintech, accountability cannot be, and exercising due diligence is imperative for the financial institutions that partner with them.

These arrangements can introduce new strategic, operational, compliance, cybersecurity, and reputational risks. Boards play a critical role in ensuring management has established an effective framework to evaluate, oversee, and monitor fintech relationships throughout their lifecycle.

Why Fintech Partnerships Matter

The pace of technological change has created pressure for financial institutions to modernize services and meet evolving customer expectations. Fintech partnerships can provide access to specialized capabilities that may be difficult or costly to develop internally.

Potential benefits include:

- Enhanced customer experience and digital capabilities.
- Faster product development and deployment.
- Expanded market reach and new revenue opportunities.
- Improved operational efficiency and automation.
- Access to innovative technologies, including artificial intelligence and advanced analytics.

While these benefits can be compelling, institutions should carefully evaluate whether the partnership aligns with their strategic objectives, risk appetite, and operational capabilities.

Key Areas of Board Oversight in Fintech Partnerships

Strategic Alignment

Directors should understand how proposed partnerships support the institution's long-term strategy and whether management has clearly defined success metrics.

Key considerations include:

- Does the partnership align with strategic priorities?
- What customer need or business objective is being addressed?
- How will success be measured?
- What are the financial implications and expected return on investment?

Risk Management and Governance

Fintech partnerships often create reliance on third parties for critical processes, data management, customer interactions, or technology infrastructure. Boards should understand how management evaluates and monitors these risks.

Areas of focus include:

- Third-party risk management processes.
- Vendor due diligence procedures.
- Ongoing performance monitoring.
- Incident escalation protocols.
- Business continuity and resiliency planning.

Regulatory Compliance

Ultimately, financial institutions remain responsible for compliance with applicable laws and regulations regardless of whether activities are performed by a fintech partner.

Boards should seek assurance that management has evaluated:

- Consumer protection requirements.
- Anti-money laundering and Bank Secrecy Act obligations.
- Fair lending considerations.
- Privacy and data protection requirements.
- Regulatory reporting responsibilities.

Data Security and Cybersecurity

Fintech arrangements often involve significant data sharing and technology integration. As cyber threats continue to evolve, directors should understand how sensitive customer and institutional information is protected.

Important considerations include:

- Information security controls.
- Data ownership and usage rights.
- Cybersecurity monitoring and reporting.
- Incident response responsibilities.
- Independent assurance reports and assessments.
- Understanding where the data is housed and managed.

Operational Resilience

Operational challenges at a fintech partner can quickly become challenges for the institution. Boards should evaluate management's plans for maintaining continuity if a partner experiences service disruptions, financial distress, or operational failures.

Questions may include:

- How critical is the partner to business operations?
- Are contingency plans established and tested?
- Is there an exit strategy if the relationship must be terminated?
- How quickly could services be transitioned to another provider?

Financial Condition and Sustainability

Many fintech organizations operate in rapidly changing markets. Boards should understand management's ongoing assessment of the partner's financial strength and long-term viability.

Areas for discussion include:

- Financial stability and funding sources.
- Growth strategy and business model sustainability.
- Concentration risks.
- Dependence on key customers or investors.

Questions Boards Should Consider Asking

As part of regular oversight discussions, directors may consider the following questions:

Strategy and Business Case

- How does this partnership support our strategic objectives?
- What problem are we solving for customers or the institution?
- What are the expected benefits, costs, and risks?

Risk and Compliance

- Has management completed comprehensive due diligence?
- How does this arrangement align with our risk appetite?
- What compliance obligations remain with the institution?

Technology and Cybersecurity

- What customer or institutional data will be shared?
- How have cybersecurity controls been evaluated?
- What independent assurance reports have been reviewed?

Governance and Oversight

- How will performance be monitored and reported?
- What metrics will be provided to management and the board?
- What escalation procedures exist for significant issues?

Resilience and Exit Planning

- What happens if the fintech experiences operational difficulties?
- Do we have a documented and practical exit strategy?
- How frequently are contingency plans reviewed and tested?

Looking Ahead

Fintech partnerships are likely to remain an important component of many financial institutions' growth and innovation strategies. Effective board oversight does not require directors to become technology experts; rather, it requires asking thoughtful questions, understanding the institution's risk exposure, and ensuring management has established appropriate governance, monitoring, and accountability mechanisms.

By maintaining a balanced focus on both opportunity and risk, boards can help institutions pursue innovation while safeguarding customers, maintaining regulatory compliance, and protecting the institution's long-term stability and reputation.

Are fintech partnerships becoming an important part of your financial institution's strategic planning? Let's talk about the risks and considerations for your institution. Contact Kristy Clark at 248-614-6446 or Kristy.Clark@rehmann.com or Liz Ziesmer at 616-975-2855 or Liz.Ziesmer@rehmann.com.

Internal Control Over Generative AI: A Board-Level Priority for Financial Institutions

Generative Artificial Intelligence (AI) is no longer just an experimental technology. Employees at financial institutions may already be using it to draft customer communications, summarize policies and contracts, support fraud and compliance workflows, analyze large data sets, and improve efficiency.

While the speed of AI creates opportunity, but it also raises a serious question for financial institutions and their boards: ***Can your organization trust Generative AI's outputs enough to rely on them?***

Generative AI is different from traditional software. While most business systems are designed to produce the same result when given the same inputs, generative AI is probabilistic, which means outputs can vary, even when prompts appear similar.

For boards and management teams of banks, credit unions, and other financial institutions, that difference creates a unique set of oversight challenges. Generative AI tools may expose confidential customer information, generate inaccurate or unsupported outputs, introduce bias into decision-making, weaken compliance processes, or create dependency on third-party vendors whose models can change with little notice.

That makes internal control over generative AI a governance priority, not just a technology issue.

How COSO Can Support AI Governance

The good news: Financial institutions do not need to invent an entirely new control model for generative AI. The Committee of Sponsoring Organizations of the Treadway Commission (COSO), a globally recognized organization dedicated to helping entities reduce fraud while improving operations and oversight, has introduced an Internal Control — Integrated Framework.

COSO's Internal Control — Integrated Framework provides a strong foundation comprising five components it deems crucial to effective internal controls in the age of generative AI. When adapted thoughtfully to your organization's unique processes, these five components can help your organization govern generative AI in a way that supports innovation and protects business objectives.

1. A Clear Control Environment

Management should define what AI use is acceptable, who owns each approved use case, how employees are trained, and when human review is required. The board should see evidence that accountability is clear across business, technology, compliance, risk, and audit functions.

2. Risk Assessment

AI risk should not be assessed in general terms. Management should classify each use case based on purpose, data sensitivity, customer impact, regulatory implications, vendor dependence, and the degree of reliance placed on AI outputs.

3. Control Activities

For higher-risk AI uses, boards should expect safeguards such as approved tools, access limits, human review, source validation, testing before deployment, change approval, prompt and output logging, and documented escalation paths.

Common control activities include:

- Human review for high-risk outputs.
- Confidence thresholds before automation is allowed.
- Approval workflows for prompts, rules, and model changes.
- Segregation of duties between those who configure and those who approve.
- Side-by-side testing before deployment.
- Source citation requirements for key outputs.
- Logging of prompts, outputs, and model versions.
- Rollback plans if performance declines.

4. Information and Communication

Boards do not need technical detail on every AI tool their institution uses, but they do need useful reporting. Management should be able to explain where AI is being used, which uses are considered higher risk, what controls are in place, what incidents or exceptions have occurred, and what assurance has been performed.

Among the questions board should ask:

- What data did the tool use?
- Which model version generated the output?
- Was the output reviewed?
- Were limitations communicated to users?
- Did anyone know the tool changed?

Organizations should maintain records of prompts, inputs, outputs, model configurations, source references, and known limitations when appropriate to the use case. They should also communicate changes clearly to the people affected.

5. Monitoring Activities

Generative AI cannot be governed with a "set it and forget it" mindset. Boards should expect management to maintain an ongoing review process, which may include tracking of:

- Accuracy rates
- Exception volumes
- Drift indicators
- Response quality
- Bias metrics
- Security incidents
- User behavior patterns

A Practical Path Forward

Financial institutions do not need to solve every AI governance issue at once. A practical first step is to establish visibility and prioritize the highest-risk uses.

Management can begin by:

1. **Inventorying current AI use cases** across departments and vendor platforms, including unofficial or "shadow AI" tools.
2. **Classifying each use case** by data sensitivity, customer impact, regulatory relevance, and business reliance.
3. **Assigning clear ownership** for AI governance, approved tools, monitoring, and escalation.
4. **Applying COSO's five components** to evaluate the control environment, risk assessment, control activities, communication, and monitoring for AI use.
5. **Reporting to the board** on higher-risk use cases, control gaps, incidents, remediation, and assurance activities.

This staged approach helps boards and management move from reactive concern to proactive governance.

Don't let your controls lag behind your AI adoption.

Evaluating where AI influences your institution's decisions, operations, and customer interactions is a critical first step — but you do not have to navigate the complexity alone. At Rehmann, we believe effective governance should do more than reduce risk. It should help financial institutions move forward with confidence, integrity, and clear business purpose. Schedule a readiness assessment with our risk advisory team today to ensure your organization moves forward responsibly and securely. Contact Jessica Dore at Jessica.Dore@rehmann.com for a personal conversation.

Proposed Revisions to Supervisory CAMELS Ratings

For the first time in 30 years, federal bank regulators are proposing a major overhaul to the CAMELS supervisory rating system, the 1–5 score regulators use to grade a financial institution's health.

CAMELS, nicknamed for the six components it evaluates — capital adequacy, asset quality, management, earnings, liquidity, and sensitivity to market risk — is the framework of the Uniform Financial Institutions Rating System, the supervisory tool the Federal Financial Institutions Examination Council adopted in 1979 to evaluate, rate, and communicate the soundness of financial institutions, as well as identify those needing heightened attention or supervisory action. .

Regulators last updated UFIRS and CAMELS in 1996, following significant shifts in financial markets, interest rate volatility, and financial instruments. This time, they're seeking to improve effectiveness and increase the public's confidence in supervisors' assessment of the banking system by modifying rating definitions and evaluation factors. Their goal: to strengthen the link between the ratings and a financial institution's safety and soundness by prioritizing material financial risks over concerns related to policies, procedures, and documentation.

CAMELS: 3 Major Changes Proposed

First, updates would align terminology with current industry standards and accounting practices. For example, references to "allowances for loan and lease losses" (ALLL) would be replaced with "allowances for credit losses" (ACL) to conform with the Current Expected Credit Losses (CECL) accounting standard adopted under U.S. GAAP in 2023.

Second, all references to reputation risk would be removed, consistent with the policies of the Federal Reserve Board, OCC, FDIC, and NCUA.

Third, updates would improve transparency by more clearly articulating expectations for financial institutions. Numerical ratings from 1 to 5 — with 1 being the highest and 5 the lowest — would remain unchanged. The proposed updated definitions for component and composite rankings are summarized below.

Proposed Changes to Component Rating Definitions

Capital Adequacy: Replace the evaluation factor concerning "the ability of management to address emerging needs for additional capital" to include consideration of "the institution's effectiveness in maintaining capital levels commensurate with its risk profile and strategic priorities through a range of economic conditions."

Asset Quality: Eliminate broad language that requires examiners to evaluate the ability of management and the board to "identify, measure, monitor, and control" risk to instead focus on evaluation of credit risks associated with a financial institution's loan and investment portfolios; foreclosed, repossessed, and other assets; and off-balance sheet exposures.

Management: Remove the sentence directing examiners to give "special consideration" to the Management component in the composite rating, ensuring supervisors take a more balanced approach. Remove factors related to "Management depth and succession," "Responsiveness to recommendations from auditors and supervisory authorities," and "Demonstrated willingness to serve the legitimate banking needs of the community," to instead focus on material aspects of risk management, as well as establish a material financial risk threshold for Management ratings of 3 or worse.

Earnings: Clarify that a financial institution's funding costs and earnings exposure to commodity prices would be considered when evaluating the quality, quantity, and trend of a financial institution's earnings.

Liquidity: Focus on "the effectiveness of funds management practices, including contingency funding plans and cash flow forecasting" to ensure a financial institution is able to maintain sufficient liquidity to meet its financial obligations in a timely manner.

Sensitivity to Market Risk: Amend the language to include an evaluation of recent net interest income performance in response to the interest rate environment, expectations for net interest income based on the balance sheet position, and exposure to interest rate volatility.

Proposed Changes to Composite Rating Definitions

Financial institutions receive a composite rating based on ratings for the components noted above, which would be redefined as follows:

Composite 1: Sound in every respect. Strong financial performance. Minor risk management weaknesses. In substantial compliance with laws and regulations. No cause for supervisory concern.

Composite 2: Fundamentally sound and no component rating more severe than 3. Satisfactory financial performance. Moderate risk management weaknesses that do not result in material financial risk. In substantial compliance with laws and regulations. No material safety and soundness concerns.

Composite 3: Some supervisory concern and no component rating above 4. Less than satisfactory financial performance or inadequate risk management practices that result in material financial risk to the institution. Significant noncompliance with laws and regulations. Requires more than normal supervision, which may include formal or informal enforcement actions. Failure appears unlikely.

Composite 4: Significant supervisory concern. Deficient financial performance. Risk management weaknesses range from severe to critically deficient. Significant noncompliance with laws and regulations that represent material financial risk. Close supervisory attention is required, including formal enforcement action. Risk of loss to the Deposit Insurance Fund or Share Insurance Fund. Failure is a distinct possibility if the problems and weaknesses are not satisfactorily addressed and resolved.

Composite 5: Highest supervisory concern. Critically deficient financial performance. Immediate outside financial or other assistance is needed for the institution to be viable. Ongoing supervisory attention is necessary. Significant risk of loss to the Deposit Insurance Fund or Share Insurance Fund, and failure is highly probable.

Potential Benefits of the Proposed Changes

The proposal could result in more efficient and effective use of management time and resources. More transparency in supervisory expectations could lead to reduced compliance costs to address any material risks, improving the institution's safety and soundness. Also, financial institutions with satisfactory CAMELS ratings have historically demonstrated higher lending and better overall bank performance, while those with poor CAMELS ratings exhibit substantially lower loan growth.

Potential Costs of the Proposed Changes

Risk management practices that do not drive CAMELS ratings or are not perceived to be directly linked to material financial risk could drop in priority. If the proposed changes delay the identification and remediation of a risk that causes the financial institution to further deteriorate and later materially affect financial condition, then the proposed changes could lead to higher costs to deal with the risk, as well as financial losses.

Public comments are due Aug. 17, 2026.
Read the proposed revisions

Stay on top of the latest developments related to CAMELS and other supervisory agency updates — get an in-depth review and evaluation of your institution's strengths, weaknesses, and opportunities, essential to guiding strategic decisions that maximize growth and earn the highest supervisory ratings. Contact Chris Plaskewicz at Chris.Plaskewicz@rehmann.com or Liz Ziesmer at Liz.Ziesmer@rehmann.com.
