



plante moran | Audit. Tax. Consulting.

Financial Institutions Advisor

Insights for 2021 and beyond



Contents

Industry spotlight: Banks and credit unions	2
Cyber resilience: Adapting to a changing cyberattack environment	4
Are your internal controls as efficient as they could be?	9
Making the right decisions: The importance of model risk management	12
Key accounting and regulatory reporting matters for 2021	14
Managing credit risk in today's environment	18
Additional content: Navigating risk & building resilience	20
Financial institutions at a glance	21
Our leaders	22



Banks

Reflecting on the past year, we've seen periods of significant volatility and concern for the health of financial institutions. The November report from the Federal Reserve points to the resilience of banks, noting capital ratios have generally returned to pre-pandemic levels even after absorbing significant losses during the year. Vulnerabilities exist due to increased leverage in businesses amid lower earnings for both households and businesses.

Household and business borrowing

Lower interest rates, the Paycheck Protection Program (PPP), and the desire to build cash reserves to weather shutdowns driven by the COVID-19 pandemic led to historically elevated outstanding debt for companies. Community banks concentrate business lending to small businesses, which have been substantially impacted by COVID-19. With the first round of PPP ending in August 2020, data from that period indicated short- and long-term delinquencies increasing to levels not experienced since 2011, demonstrating the significant reliance of small businesses on PPP loans. Household debt levels have also increased, although mostly in loans to those with prime credit scores (720+). Near-prime and subprime borrower loan balances continue to be lower than pre-recession levels. Mortgage debt makes up two-thirds of all household debt, and forbearance and loss-mitigation measures introduced in the spring of last year have softened the effect of COVID-19 on mortgage delinquencies. Increases in real estate values have also resulted in lower levels of overall housing leverage when compared to the last 10 years.

Primary concerns in the near term

The ongoing pandemic and its consequences top the lists of near-term risks. While many forecasts predict a moderate recovery in our economy, delays in distribution of vaccines will have an impact, especially if there are shutdowns and layoffs. Nonbank financial institutions with higher leverage, including hedge funds and life insurance companies, may be more exposed to sharp drops in asset values and volatility in funding risks. The banking sector continues to be moderately capitalized.

Our take

Community banks met the challenges of the COVID-19 pandemic head-on. With significantly higher than normal loan volumes stressing internal systems, banks managed to fund more PPP loans in 45 days than the number of loans they'd see in a typical year. In addition, mortgage volumes and enhanced spreads led to good profitability for the year, and many borrowers remained current with their obligations. We expect continued focus on internal controls and cybersecurity due to changes put in place for a remote work environment, increased mortgage volume, and new product offerings. As government programs wind down, monitoring asset quality and financial statements should be prioritized to quickly identify potential problem credits.



Credit unions

2020 will long be remembered as the year of change for credit unions, given the shifts in operations, member service models, budgets, and balance sheets. Yet, credit unions haven't only survived these changes but embraced them and are thriving. As an industry, credit unions have grown membership, assets, and net worth and remain well-positioned for 2021 and beyond.

Lending update

While some member behavior did change during 2020 and the introduction of PPP loans grew many credit unions' member business loan (MBL) portfolios, overall loans increased \$69 billion or 6.3% from September 2019 to September 2020. (December information not available at time of writing.) Commercial loans saw the largest increase at 16.8% but still remain a small percentage of credit union portfolios. Loans secured by 1–4 family residential properties saw the most significant dollar growth, increasing by \$42.1 billion or 9%. This is in addition to the significant sales volume seen on many income statements. Auto loans, while increasing a net 1.2%, saw a dichotomy: Used auto loans increased 4.4%, and new auto loans decreased 3.7%. Interestingly, credit card balances declined 4.9% year over year as consumer spending declined and savings increased. As of Sept. 30, 2020, overall delinquency was down to 55 basis points compared to 66 basis points a year ago. Net charge-offs saw a similar decline.

Supervisory priorities

The NCUA shed some light on their examination focus areas for 2021. Within the allowance for loan and lease losses (ALLL) area, NCUA has indicated a temporary shift from CECL preparedness to a more fundamental ALLL methodology review, including a deeper dive in overall credit risk management. CARES Act compliance, BSA/AML compliance, and overall consumer financial protection will continue to be priority areas. Cybersecurity remains important, and NCUA will look to roll out its new InTREx platform for IT reviews. Liquidity has also been identified as a focus area, specifically managing the eventual outflow of member deposits that flooded most credit unions this past year.

Our take

The state of the industry is strong but not without headwinds in 2021. We expect additional regulations, economic challenges, and continued hurdles posed by remote staffing, partially closed branches, and increased cyberthreats, among others. Strong internal controls, policies, and risk management programs are paramount as is strong, strategic leadership, but the industry's strong footing will provide a position of strength.



CYBERSECURITY

CYBER RESILIENCE:

Adapting to a changing cyberattack environment



Jennifer Fiebelkorn

Principal

jennifer.fiebelkorn@plantemoran.com

Perpetrators of cyberattacks threaten daily to infiltrate your systems with malicious intent. A cyber resilience strategy can help you withstand attacks and minimize business disruption to protect your data — and your profits.

If you're like many of our clients, the notion of a "cybercriminal" and the term "cybercrime" conjure up the image of a rogue teenager hiding out in their parent's basement, hacking on their computer for hours on end. Most cybercrimes are considered threatening rather than devastating, primarily causing headaches and inconvenience, but not overly disruptive to an organizations' ability to operate.



Ben LeClaire

Senior Manager

ben.leclaire@plantemoran.com

Unfortunately, that impression is not reality. The cybercriminal and cybercrime landscape has vastly changed. We're dealing with organized cybercrime groups that function with business plans, operating protocols, organizational structures, and strategies that mirror the formats of some of today's most successful and ethically run organizations. Their resources, expertise, attack sophistication, and hacking toolkits continue to grow as does the volume and severity of cyberattacks against organizations. History has shown that cybercriminals pose significant threats, and their mechanisms can and have resulted in devastating impacts to organizations.



Matt Babicz

Manager

matt.babicz@plantemoran.com

Notable examples of cyberthreats that impacted financial institutions in 2020:



RANSOMWARE

Cybercriminals repurposed the traditionally known ransomware attack by replacing some of the typically automated processes with targeted manual processes. Rather than releasing a virus that auto-encrypted (locked) all of the financial institution's files, the hackers found a foothold on the network, sat quietly, and worked to identify the most critical, sensitive, and business proprietary information and systems before initiating the attack. Once identified, the hackers deleted all backup files then quickly encrypted the sensitive files and systems previously identified. The ransom requested was 2 bitcoin or around \$65,000 at the time of execution.



WIRE FRAUD

Cybercriminals identified the protocol that the financial institution's customers were required to follow to initiate a Customer Information File (CIF) change. This was done by calling the institution periodically over the course of a few weeks and inquiring about the wire transfer and CIF change processes. The attackers then changed customer email addresses on file, leveraged the newly added email addresses, and initiated multiple wire transfers, successfully stealing more than \$500,000.



PAYROLL SYSTEM COMPROMISE

Cybercriminals strategically compromised a user account from the financial institution's cloud-based payroll system with privileged access, giving the new user account creation capabilities. When leveraging the account at its authority level, the attacker created several new accounts that emulated standard new hire employees with typical job titles, appropriately tailored salaries, personal information, etc. This was all done without detection. Payroll jobs were created, and paychecks were scheduled in alignment with the institution's normal payroll cycle. Although the institution detected the incident shortly after the first payroll cycle, losses incurred totaled roughly \$250,000.



BUSINESS EMAIL COMPROMISE

The cybercriminal's goal was to hijack the targeted financial institution's process for requesting, authorizing, and administering wire transfers. Over a short period of time through reconnaissance, the bad actor gathered information identifying the institution's email-naming convention, their personnel with capabilities to request and authorize wire transfers, and then compromised and leveraged a customer's account to request a \$1,000,000 wire transfer. With the compromised institution's email address and understanding of the approval process, the attacker was able to successfully circumnavigate the process and wire the amount requested.

While traditional tactics of phishing and malware are still the most common cyberattack methods, the next wave of cyber criminals can quickly pivot to other, more technical, methods to exploit vulnerabilities and disarm your defenses. The result can be total business disruption. So, what's your best defense? An evolving cyber resilience strategy that allows you to mitigate the threats of a cyberattack and enhance your ability to respond and recover from an attack.

Cyber resilience allows you to adapt to a changing cyberthreat environment

Cyber resilience goes beyond preventing or responding to a breach — it's your ability to operate during, adapt to, and recover from a cyberattack (the word "resilience" is the key here). If your organization has a high level of cyber resilience, a cyberattack is much less likely to hamper your business operations — you'll be able to protect your data, reduce the impact of business disruption, and prevent devastating revenue loss.

We've entered a new digital era — institutional leaders and regulatory agencies need to continue to evolve their idea of effective cybersecurity beyond defense and reaction. By continuing to evolve, these organizations will be able to anticipate attacks and have stronger mechanisms in place to identify attacks and not only recover technologies more effectively and efficiently, but continue business during an incident or disaster.



STEP 1: IDENTIFY YOUR MOST CRITICAL INFORMATION AND ASSETS.

The evolution of cloud-based solutions, including the Internet of Things (IoT), remote workforces, and vendor integration into organizations' process and systems means that organizations must be smarter and more diligent about securing customer information as well as how critical data assets are shared and consumed. A critical data asset is data that, if lost, stolen, or threatened, would cause significant damage to your revenue, reputation, and ability to run day-to-day operations.

There's a misconception that all data needs to be protected equally, but consider this: What data would be most valuable to a cybercriminal? You can identify critical assets using **cyber risk assessments** and IT audits. Once your critical data assets are identified and their value is measured, you can partner with an external expert to create a process that appropriately protects against fraud and breaches.

Examples of critical data assets:





- ✓ Client confidential information
- ✓ Sensitive staff information & data
- ✓ Corporate financial data
- ✓ Key business systems (inhouse, outsourced, & hosted)
- ✓ Sensitive/proprietary information
- ✓ Data custodians (internal & external)



STEP 2: ALIGN YOUR CYBER RESPONSE AND PREPAREDNESS STRATEGY TO THE CURRENT THREAT ENVIRONMENT.

If you're not keeping up with the latest methods to identify and prevent cybersecurity breaches, prepare to be attacked. Many organizations still rely on out-of-date security measures, like policies, procedures, and passwords that address decades-old threats. While it can seem like a difficult task to keep track of all possible cybersecurity threats, you should at least update your threat intelligence and vulnerability management strategies to address and stay current with today's most common threats — ransomware, malware, unauthorized access to your email system, weak users, and loss of data or hardware.

Key actions to take to mitigate risk and respond to current cybersecurity threats:

-  Identify current threats and act on intelligence.
-  Prioritize cyber risks — you can't defend against all possible risks, order risks in terms of probability, and impact.
-  Focus less on specific technologies, since these are continually evolving, and more on security goals as they relate to your overall strategic plan and mission.
-  Make sure your people, processes, and technologies are all protected — cybersecurity is an organization-wide responsibility, and not just through an IT department's efforts and processes.

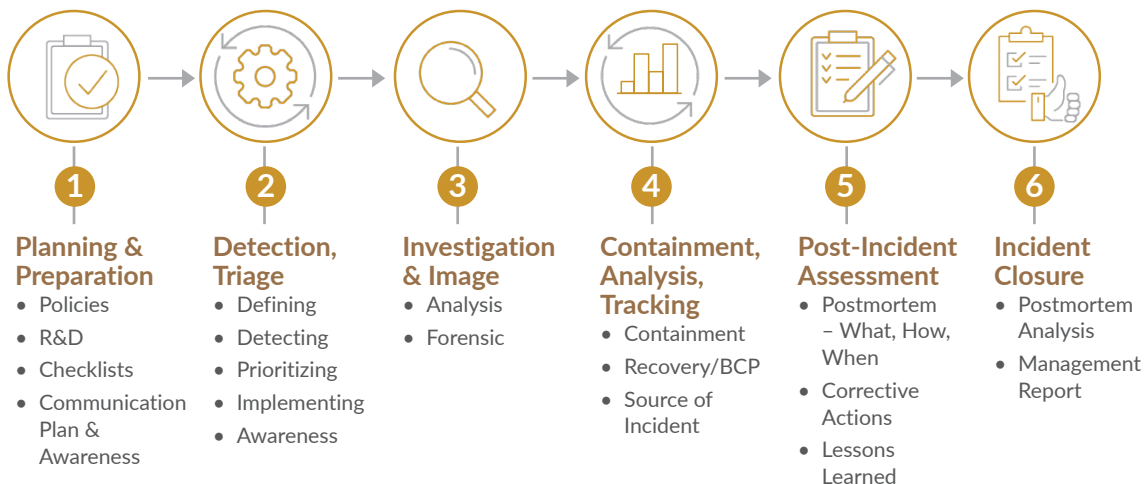
3

STEP 3: DEVELOP AND SIMULATE CYBER INCIDENT RESPONSE STRATEGIES.

Next, your organization should have a tested program in place to respond to a cybersecurity incident. Without a formal plan, your customers, employees, IT systems, and even brand can be negatively impacted. Identify a cybersecurity incident response team that will activate when security breaches occur to mitigate their impact on your organization. Your incident response team should include representatives from all major departments, along with internal or external legal counsel.

Here's how to create and maintain an incident response plan:

- 1 Review and update policies, prepare checklists, communication strategies, and templates for internal and external parties.
- 2 Establish a process to detect and triage security events, including defining event types and actions to follow for each type of event, from nuisance to data breach.
- 3 Investigate and analyze a breach that includes assistance from forensic examiners, cyber professionals, and cyber insurance agents to determine the origin of when the attack occurred and potential impact zone.
- 4 Contain the incident to prevent further damage, and enact business continuity or disaster recovery plans as needed.
- 5 Complete a post-incident assessment to identify correction actions and lessons learned.
- 6 Prepare a documented summary of event and report lessons learned, and update policies and plans as needed.





Uninformed users can jeopardize an entire system. Therefore, cyberthreat awareness training is imperative to help users identify threats to information security and take proper action



STEP 4: FOCUS ON A CULTURE OF AWARENESS.

Finally, increase awareness and vigilance among your staff. An essential factor in data security is human behavior. Uninformed users can jeopardize an entire system. Therefore, **cyberthreat awareness training** is imperative to help users identify threats to information security and take proper action in response. All users need to stay up to date on the latest types of attacks.

Security awareness training helps mitigate these top security breaches:

- ✓ Targeted ransomware
- ✓ Phishing attacks, beyond just email
- ✓ Mobile device attacks
- ✓ Cloud & wireless attacks

As cyberattacks grow more sophisticated, complex, and financially devastating, don't sit and wait for support from your examiners, proactively work on preventing them! Cyber resilience allows you to embrace disruption safely and operate while under persistent threats and sophisticated attacks. You can't anticipate every possible cyber risk, but we can help protect your organization with forward-planning and improved cyber safeguards.



INTERNAL CONTROLS

Are your internal controls as efficient as they could be?

Both ineffective and inefficient, management review controls are an impediment to a growing financial institution. As an audit team serving financial institutions, we get to see a variety of our clients' internal control frameworks. Some have been in place for 50 years and others, at fast-growing, newer companies, are still maturing into a comprehensive control framework. While there are some degrees of variability in how controls are documented, we're continually surprised that each of our clients have almost the exact same controls. We've always considered this to be a function of the following attributes:



GROUPTHINK

More than most other industries, financial institutions are cross-pollinators. Members of management take experiences from one employer to another, and much of their training is received from industry groups or consultants that also have perpetuated a "status-quo" mentality.



SERVICE PROVIDER LIMITATIONS

The consolidation of technology processing systems has limited the ability of individual institutions to challenge the status quo.

As such, many rely heavily on management review controls (MRCs), which are almost always detective controls executed by staff to ensure their financial reporting is accurate.



Kyle Manny

Partner

kyle.manny@plantemoran.com



Kate Krones

Manager

kate.krones@plantemoran.com



Joe Oleksak

Partner

joe.oleksak@plantemoran.com



It's up to bold management teams to sit down and consider what they could do to improve their internal control systems.

An example of an MRC is the process by which a staff member verifies all critical changes to loan accounts are authorized and accurate. This control detects errors or unauthorized changes made by loan processing or operations teams during the loan boarding and maintenance processes. While this process is prevalent at all of our clients, it's inherently flawed for the following reasons:



SYSTEM REPORTS

System maintenance reports are often clunky and voluminous. These standard reports were designed by the core system providers to present all customer account-level changes, regardless of importance, which proved very challenging to use as organizations grow.



CUSTOM-BUILT REPORTS

Many clients have developed reporting on account-level changes using a secondary report writing software. While workarounds exist, they create significant burden on system administrators to ensure customized reports are complete and accurate and need to be tailored and tested every time changes are made to products or services.



HUMAN ERROR

This process requires an employee to (1) understand what he/she is responsible for reviewing, (2) research whether each change was authorized and accurate, and (3) document his/her review. We identify many errors in both the execution and documentation of those three responsibilities of the control operator.

The solution is preventive application controls

The systems used by financial institutions are incredibly sophisticated software platforms and, yet, most financial institutions haven't effectively controlled the ability to input or modify information that impacts financial reporting. Many institutions justify this lack of system control because they fear customer experience may be impacted. We can hear a chief operating officer say, "I can't restrict the ability to change customer information because we have some customers that don't use online banking." Our response to that statement is, "Well, have you considered restricting bank-employee access to make changes to customer information for customers that do use online banking?" At a minimum, you'd have fewer changes that would require management review. If all customer account changes were required to be made by customers, you'd completely remove the risk of internal fraud related to this process and further justify the investments many have made in customer fraud detection systems. There are endless examples of application controls you could implement to reduce the risk of failure of MRCs; however, it's up to bold management teams to sit down and consider what they could do to improve their internal control systems. There will always be a need for certain MRCs within a strong internal control system. The reliance upon such controls hasn't kept up with changes in terms of business operations and technological investments.

Successful identification and implementation of preventive application controls can really move the needle in the following ways:



MORE TIMELY, RELIABLE FINANCIAL REPORTING

Errors won't go undetected and processing time for changes made as a result of the MRCs is eliminated.



ABILITY TO SCALE OPERATIONS

Removing some of the "process" within the production cycle allows financial institutions to scale without making additional investments in human capital.

As described above, there's a strong case to be made that the implementation of automated application controls will positively impact the reliability of information and improve the bottom line. Management teams certainly need to weigh the benefits against some challenges, which will be created through the limitation of flexibility and potential impact to customer experience.

Don't take our word for it. Here's what the Institute of Internal Auditors says: "One of the most cost-effective and efficient approaches organizations use to manage [transactional] risks is ... the use of controls that are inherent or embedded (e.g. three-way match on account payable invoices) into transaction support applications as well as controls that are configurable (e.g. accounts payable invoice tolerances)."

We encourage all financial institutions to recognize where they are reliant on MRCs and challenge their operations teams to identify where application controls could be developed to render certain MRCs obsolete. If your team needs help systemically reviewing your business processes, we can assist. Our team of cybersecurity and IT auditors are uniquely qualified to challenge the "status quo" to modernize your key controls and empower you to grow your financial institution profitably.



We encourage all financial institutions to recognize where they are reliant on MRCs and challenge their operations teams to identify where application controls could be developed to render certain MRCs obsolete.



MODEL RISK MANAGEMENT

MAKING THE RIGHT DECISIONS:

The importance of model risk management



Bryan Johnson

Principal

bryan.johnson@plantemoran.com

With the increasing use and reliance on technology, automated predictive, economic, and financial models help financial institutions make faster and better business decisions. But how should organizations manage risks? A strong model risk management (MRM) framework is critical.

Over the past several years, a number of financial institutions have embraced the use of automated predictive, economic, and financial models to conduct financial and business analyses. Many are also in the process of developing or implementing credit loss models to address the Financial Accounting Standards Board's new current expected credit loss (CECL) standard.



Steve Schick

Partner

steve.schick@plantemoran.com

Increasing model use, increasing risks

The proliferation of data and the increasing complexity of financial analyses have caused many financial institutions to turn to models to help increase efficiencies, reduce mundane and repeatable tasks, and save time and resources. While the use of models allows financial institutions to make faster and better business decisions, they also present significant risks if a strong MRM framework isn't in place to govern their use.

The challenge is that few small and medium-sized financial institutions have robust model risk management processes to govern their use of models. While financial institutions in excess of \$10 billion are subject to model risk management regulatory guidance, smaller financial institutions don't have the same obligations — although MRM is encouraged. This has led many to approach model implementation on an ad-hoc basis, with functional areas developing models in order to enhance their specific decision-making processes. The issue with this ad hoc approach is that it opens an organization up to a wide range of risks, including risks associated with input accuracy, data completeness, and alignment of bank-specific assumptions and strategic goals.

Making model risk management a priority

While smaller institutions might not be subject to the same regulations as their larger counterparts, this doesn't mean they should ignore such requirements altogether as they may be subject to such MRM requirements in the future. Additionally, if they're going to spend the time and resources developing and implementing models, financial institutions should make sure those models work as intended. The last thing any financial institution wants to do is rely on inaccurate models for making key business decisions.

Where to start?

Financial institutions that use predictive, financial, or economic models should consider enhancing their approach to MRM. As a starting point, this could include undertaking the following key activities:



Create an inventory of existing models

It's important to conduct an inventory of any existing or in-development models. As a part of this, be clear as to the difference between a model and a tool so that all stakeholders have a common understanding of how to use and contribute to the inventory. In connection with documenting the inventory, include each model's purpose, model owner, data sources, and significant assumptions.



Understand regulatory requirements related to model use and verification

Financial institutions should take time to understand the regulatory requirements related to model development, implementation, and use, including validation, even if they're not currently required to be in compliance. This understanding will help the organization manage the organization's entity-wide risk and help them establish MRM processes aligned to comply with regulations they may be subject to in the future.



Test and validate models

Institutions should test and validate any significant or complex models before implementation and on an ongoing basis so management can be confident in model outputs. For example, before implementing a new model, it should be run parallel with the existing process to ensure the new model is operating as intended and in line with expectations. On an ongoing basis, the model's accuracy should be tested to determine if the use is still appropriate given the potential change in facts and circumstances. As recommended in the regulatory guidance, model testing and validation should be conducted by individuals or a third party independent from the models' users and those that developed it. Based on the results of the testing process, institutions can identify model errors, track corrective actions, and ensure appropriate use.

Note: Financial institutions should validate their use of the third-party models. This would include determining whether a model is appropriate for its intended use and that any customizable model assumptions are accurate and relevant.



Involve the right stakeholders

MRM should be an entity-wide activity. The board should be responsible for providing governance of the entire MRM process, while management should be tasked with developing the MRM framework and related processes. Leaders with insight across the organization should be engaged in the MRM process to ensure assumptions are appropriate, model documentation is robust, and data sources are valid and accurate.

Knowing you're making the right decisions

Models can be instrumental in driving better business decisions or your financial reporting process — but only if you're able to rely on the outputs. If you would like more information on our model validation services or how we can enhance your MRM framework, please contact your local Plante Moran business advisor.



ACCOUNTING AND REGULATORY UPDATES

Key accounting and regulatory reporting matters for 2021



Ryan Abdoo
Partner

ryan.abdoo@plantemoran.com



Kate Krones
Manager

kate.krones@plantemoran.com

With 2020 in the rearview mirror, the financial institutions industry heads into 2021 facing several key financial reporting changes. Here are the top four your financial institution should prepare for now.

Current Expected Credit Losses (CECL): Changes to the measurement of loan losses

Perspectives on those that adopted in 2020

Calendar year 2020 was an adventure for many financial institutions, not only due to the COVID-19 pandemic but also because of the adoption of CECL. The bad news for adopters? Implementation turned out to be more time-consuming and costly than originally anticipated. But there was also some good news. First, institutions yet to adopt CECL are not required to have the same complex models as institutions that were already required to adopt CECL. And second, institutions that adopted last year encountered few issues with the level of their reserves.

The common issues experienced were mainly focused on the documentation supporting the calculation, and include:

- ✓ The “journey memo.” In the years leading up to adoption, many checks and balances were performed and decisions made along the way that may or may not have been documented. This documentation provides the roadmap for the institution’s adoption of this new accounting standard.
- ✓ Assumptions used as a result of historical data that did not include a full economic cycle.
- ✓ The determination of assumptions for the forecast period.
- ✓ The methodology for reversion.

The path for those yet to adopt CECL

In November 2019, the Financial Accounting Standards Board (FASB) approved the delay of several major accounting standards, including a delay of CECL implementation to January 2023 for calendar-year entities. This change was the first indication of the board’s shift in mindset to an environment where large, public companies adopt new standards multiple years before smaller institutions. However, in the wake of the COVID-19 pandemic, some institutions haven’t made as much progress toward CECL adoption as they would have liked. Accordingly, many are looking to make up ground in 2021 by taking next steps such as selecting a model, evaluating historical data, performing dry runs, and calibrating their calculations for implementation.

To assist your institution in working toward CECL adoption, here’s a suggested timeline to consider:

Calendar year 2021

- 1 Assess and understand available methodologies
- 2 Identify available data
- 3 Assess data limitations against available methods
- 4 Select your methodology
- 5 Organize and validate data
- 6 Finalize segmentation
- 7 Establish processes and controls

Calendar year 2022

- 1 Verify new data activity
- 2 Perform shadow calculations
- 3 Calibrate model accordingly
- 4 Finalize controls
- 5 Test controls
- 6 Have model validation performed
- 7 Measure impact as of Dec. 31, 2022, and record variance to equity



In November 2019, the Financial Accounting Standards Board (FASB) approved the delay of several major accounting standards, including a delay of CECL implementation to January 2023 for calendar-year entities.



It's important for an institution to first identify affected credits, effectively quantify the change in cash flows and, lastly, ensure their bases are covered from an accrual status perspective.

Remaining modified loans: Classification and accrual status

While Congress and regulatory agencies have granted relief from the application of the highly subjective and challenging topic of troubled debt restructures (TDRs), institutions are reminded they're not exempt from properly classifying and evaluating accrual status.

Overall, financial institutions have provided a wide range of loan modification programs with varying degrees of success. And while it appears that the majority of modified loans have returned to making regular payments under the contractual terms of the obligation prior to the modification, numerous institutions continue to have a material amount of loans that have not. In these instances, it's important for an institution to first identify affected credits, effectively quantify the change in cash flows and, lastly, ensure their bases are covered from an accrual status perspective. As part of this assessment, institutions should ask and answer the following questions for loans that remain on modified terms.

- ❓ What is the nature of the borrower's business?
- ❓ How much disruption has the borrower's business experienced due to the pandemic?
- ❓ Does the current debt service coverage ratio support the collection of both principal and interest payments that existed prior to the first modification?
- ❓ Is there a valuation of collateral that accounts for the post-COVID-19 environment?
- ❓ How much equity (deficiency) exists with the collateral?
- ❓ Are there other mitigating factors that might remove doubt of collectability of both principal and interest (e.g. substantial guarantor net worth and verified liquidity)?

The ultimate purpose of these questions is to gather and weigh both positive and negative evidence associated with collecting both principal and interest, collectively and individually. While the ultimate determination of accrual status can be one of judgment, institutions should be prepared to defend and support those conclusions with appropriate documentation.

Guide 3 disclosure changes

The Securities and Exchange Commission (SEC) has adopted updates to statistical disclosure requirements for banking registrants to clarify the scope and amended current reporting periods and disclosure requirements. The updates clarify that these disclosures are required for all banking registrants and generally streamline the required disclosures in an effort to improve the quality of information provided to investors. For example, the amended rules remove the five-year historical disclosure period and align with the periods and information presented in the financial statements. Bank holding companies are required to comply with the updates for fiscal years ending on or after Dec. 15, 2021, and early adoption is permitted.

Reference rate reform

The countdown is on: the industry now has less than a year until the sunset of LIBOR at the end of 2021. Many financial institutions are still in the early phases of determining their exposure to this index and developing a transition plan. Here are some key action items to consider as your institution prepares for the transition:

- ✓ Review existing contracts and agreements for the use of LIBOR to identify areas of exposure and any fallback language that may already exist. Common areas include loan, securities, interest rate swaps, debt, and leases.
- ✓ Identify a new reference rate (many institutions are looking to the Secured Overnight Funding Rate (SOFR), Ameribor, or Bank Yield Index), educate the lending team and others within the organization on key differences between the indices, and establish a date for the transition from LIBOR for new agreements during 2021.
- ✓ Develop and execute a plan to transition existing contracts and agreements to a new reference rate.

2021 is set to be another challenging year for financial institutions as the industry continues to face uncertainties from COVID-19, challenges with CECL adoption, and the implementation other significant financial reporting measures. If you have questions, give us a call.



2021 is set to be another challenging year for financial institutions as the industry continues to face uncertainties from COVID-19, challenges with CECL adoption, and the implementation other significant financial reporting measures.



MANAGING CREDIT RISK

Managing credit risk in today's environment



Brian Franey
Partner

brian.franey@plantemoran.com



Kevin Garcia
Senior Manager

kevin.garcia@plantemoran.com

Financial institutions are under a significant amount of pressure. They're constantly working to balance risks and opportunities in order to manage their portfolios and drive future growth.

Below, we highlight the increased risks in the leveraged lending market and suggest activities that can help financial institutions ensure they're managing their risks effectively.

Leveraged lending market

The leveraged lending market has seen increased stress over the past year, with significant impact from the effects of COVID-19 and new concerns still emerging. Leveraged lending refers to a transaction where the borrower's post-financing leverage, when measured by debt-to-assets, debt-to-equity, cash flow-to-total debt, or other such standards unique to a specific industry, significantly exceed industry norms for leverage.

Increasing market stress

The U.S. leveraged loan default rate is expected to increase to 4.76% by the end of 2021 from its current level of 3.89%. The default rate peak is expected at less than 6%, but the default cycle could extend for another one to two years. Balance sheet maneuvers, specifically covenant waivers and extensions, are expected to remain elevated.

For industry sectors, market participants expect relative performance to be better for the technology, healthcare, communication services, and consumer discretionary sectors. Conversely, higher risks are seen in the retail, oil and gas, and leisure/lodging sectors.

Growing risk for leveraged lending

As a result of various economic and market issues, banks and other financial institutions have seen an increase in defaults within their leveraged loan portfolios. This has led to a tightening of credit within the leveraged lending market.

This is somewhat of a reversal from a year or two ago when community banks were looking to get into leveraged lending. Now, financial institutions are pumping the brakes — tightening up credit underwriting and suggesting that the market may experience a downturn in the short term.

What can financial institutions do to mitigate leveraged lending risks?

For financial institutions with leveraged lending portfolios, mitigating risk will become a major factor in success, particularly if market stress continues well into 2021. In order to manage risks more proactively, financial institutions should monitor their borrowers' financial performance more closely. This could include activities, such as:

- ✓ Reviewing financials more frequently than in the past, such as reviewing a borrower's financial results quarterly rather than annually.
- ✓ Increasing scrutiny with accounts receivables, inventory and fixed asset capitalizations are monitored effectively to ensure credit quality is maintained, and that losses and delinquencies do not mount.
- ✓ Monitoring accounts payables listings to ensure the borrower is not extending terms with vendor relationships.
- ✓ Conducting more frequent meetings or site visits (i.e. biannually rather than annually or every 18 months) with borrowers to ensure the institution fully understands the customers business, any new business ventures that the customer is expending cash on not included in the lending relationship that could place stress on the balance sheet, as well as further understanding the key and their actions to mitigate risks related to their line of business.
- ✓ Financial institutions that take the time to strengthen their monitoring of higher risk borrowers will be better able to manage more volatile market conditions and decrease the likelihood of future losses occurring.

Managing your risks to create new opportunities

We've worked with numerous banks and credit unions to manage and evaluate credit risks. If you'd like more information on leveraged lending concerns or additional credit risks, please contact your local Plante Moran business advisor.



Financial institutions that strengthen their monitoring of higher risk borrowers will be better able to manage more volatile market conditions and decrease the likelihood of losses.



ADDITIONAL CONTENT

Navigating risk & building resilience

The COVID-19 pandemic has created a critical need for financial institutions to reevaluate how they are navigating risk. Check out our additional content relevant to key areas impacting financial institutions.

Key areas of focus:

Content to guide and inform you:



Need to stay ahead
of audit and technical
accounting regulations
and changes as well as
risk mitigation strategies



Enhanced concerns
around credit
risk/loan review



Increased reliance
on model risk
management and
CECL implementation



Heightened cyber risk
and the critical need to
protect consumer data

Receive relevant content in your email — **subscribe now** to our Financial Institutions Perspectives.

For more insights from our experts, visit:

Our thinking webpages for and



AT A GLANCE

Financial institutions

Grounded, practical, bottom-line focused

The pressure on today's financial institutions is relentless. Managing rapidly changing regulations, complex reporting requirements, and cybersecurity risks can be challenging, but our team of specialists provide seamless service, a customized approach, and pragmatic solutions to address these challenges and more. Our key services include:

- Financial statement audits
- Tax planning & strategies
- Internal audits
- Regulatory compliance & BSA reviews
- Loan review
- IT assurance services
- Incident response
- Cybersecurity
- ITGC & GLBA assessment
- Network security
- Social engineering
- Operations consulting & improvement
- Human resource effectiveness & employee benefits consulting
- CECL implementation
- Real estate advisory
- Capital raising & M&A transactional support & due diligence
- Valuation services including financial instruments, intangible assets, loans, & deposits
- Model risk management
- FDICIA implementation

Client profile

✓ 500+

financial services clients

✓ 150+

financial institution clients served by risk management practice providing outsourced or co-sourced internal audit services

✓ 275+

financial institutions clients



Clients range in size from small institutions with less than \$100 million in assets to national institutions, many of which are SEC registrants and FDICIA-compliant



Practice profile



20 partners

200 industry professionals

50+ years serving financial institutions

Industry involvement



NATIONAL ASSOCIATIONS

- American Bankers Association
- Independent Community Bankers of America
- Bank Director
- Financial Managers Society
- Information Systems Audit & Control Association
- International Information Systems Security Certification Consortium
- AICPA National Banking & SEC Conferences
- AICPA NCUA National Credit Union Conference
- Association of Credit Union Internal Auditors
- Credit Union Executive Society
- National Association of State Credit Union Supervisors
- Credit Union National Association CFO Conference

STATE ASSOCIATIONS

- Indiana Bankers Association
- Colorado Bankers Association
- Michigan Bankers Association
- Community Bankers Association of Michigan
- Michigan Credit Union League
- Ohio Bankers League
- Ohio Credit Union League
- Illinois Bankers Association
- Community Bankers Association of Illinois
- Iowa Bankers Association
- Wisconsin Bankers Association



OUR LEADERS

**Brian Pollice**

CPA | Audit partner

brian.pollice@plantemoran.com

Brian leads Plante Moran's financial services practice.

**Ryan Abdoo**

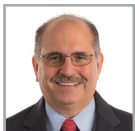
CPA, CGMA | Audit partner

ryan.abdoo@plantemoran.com

**Rob Bondy**

CPA | Audit partner

robert.bondy@plantemoran.com

**Kevin Conte**

CPA | Audit partner

kevin.conte@plantemoran.com

**Jeannette Contreras**

CPA | Tax partner

jeannette.contreras@plantemoran.com

**Brian Franey**

CPA | Audit partner

brian.franey@plantemoran.com

Brian leads Plante Moran's financial institutions practice.

**Theresa Greenway**

CPA, MST | Tax partner

theresa.greenway@plantemoran.com

**Brian Howe**

CPA | Tax partner

brian.howe@plantemoran.com

Brian leads Plante Moran's financial institutions tax practice.

**Sherrie Krowczyk-Mendoza**

CPA, CFSA, CRP | Audit partner

sherrie.krowczyk-mendoza@plantemoran.com

**Kyle Manny**

CPA, CGMA | Audit partner

kyle.manny@plantemoran.com

**Joe Oleksak**

CRISC, CISSP | Consulting partner

joe.oleksak@plantemoran.com

Joe leads Plante Moran's financial institutions technology/cybersecurity practice.

**Kenley Penner**

CPA | Audit partner

kenley.penner@plantemoran.com

**Scott Phillips**

CPA | Audit partner

scott.phillips@plantemoran.com

**Chris Ritter**

CPA | Audit partner

chris.ritter@plantemoran.com

**Steve Schick**

CPA, CGMA | Audit partner

steve.schick@plantemoran.com

**Troy Snyder**

Consulting partner

troy.snyder@plantemoran.com

Troy leads Plante Moran's financial institutions regulatory compliance practice.

**Michelle St. Ours**

CPA | Tax partner

michelle.stours@plantemoran.com

**Karla Whittenburg**

CPA | Audit partner

karla.whittenburg@plantemoran.com

Financial Institutions Advisor

This publication is distributed with the understanding that Plante & Moran, PLLC is not rendering legal, accounting, or other professional advice or opinions on specific facts or matters and, accordingly, assumes no liability whatsoever in connection with its use. Please send change of address or additions/corrections to the mailing list to jenna.mcclelland@plantemoran.com.