plante moran | Audit. Tax. Consulting.

Financial Institutions Advisor

Insights for 2022 and beyond

Contents

INDUSTRY SPOTLIGHT

Banks

Over the past 12 months, the banking sector has continued strong profitability with a 12.66% return on equity through Sept. 30, 2021, and positive operating income growth for the first time since 2008. The November financial stability report from the Federal Reserve points to a recent rebound in net interest margin from the record low in June of 2021. Both noninterest income and expenses have increased. While insured institutions recorded the third consecutive quarter of negative provisioning expense, overall allowance levels as a percentage of loans remain higher than pre-pandemic levels, as net charge-offs declined further to record lows.

Household and business borrowing

Low interest rates, ongoing government support, and improved earnings have allowed small businesses to decline overall borrowings. Delinquencies on mortgages and consumer debt, which fell early in 2020, have remained below pre-pandemic levels. As the economy continued to reopen in early 2021, consumers also increased borrowings on mortgages, credit cards, and auto. Additionally, the expiration of assistance programs have increased the risk of additional financial stress in upcoming quarters.

Banking health

Through late 2020 and throughout 2021, banks have increased capital levels and remain well-capitalized. Credit risk remains elevated; however, the Federal Reserve removed restrictions on capital distributions for large banks in June 2021. With significant deposit growth over the past 12 months, liquidity risk and the risk of maturity mismatch remain low from the perspective of the Federal Reserve, as banks continue to have high levels of liquidity and stable funding.

Primary concerns in the near term

Positive outlooks and better-than-expected economic data through 2021 have supported high asset prices; however, the ultimate extent and duration of the pandemic remain one of the more significant risks in the financial system. Despite the pandemic's role in the risk landscape, persistent inflation and monetary tightening are being identified by banks more frequently when looking for risks associated with the next 12–18 months. (Source: FDIC)

Our take

Community banks have remained a pillar of the small business economy. Many banks have excess liquidity stemming from deposit growth and are carefully evaluating asset classes for possible investment. Mortgage banking activities and the final stages of the PPP loan program have continued to support profitability. As staff return to the office full time, the slowdown in loan demand is a welcome opportunity to get caught up on project backlogs. For leaders, now is the chance to reinvest in your talent. While the Federal Reserve didn't mention anything significant about the "great resignation," businesses in all sectors are seeking strong candidates that fit requirements and culture. Last year, we warned of asset quality challenges warranting additional monitoring. We continue to keep that high on the list of things to worry about over the next two years. Now is a good time to connect with your customer, understand their financial well-being, and stress their financial results: How well do they weather a significant spike in interest rates? How is their supply chain?

Credit unions

Following an unprecedented year in 2020, 2021 saw a partial return to normalcy for many credit unions' operations. Many questions that were foremost in executive's minds coming into the year have been answered, at least for now. Deposit runoff hasn't occurred as expected, loan losses have been significantly lower than most feared entering the year, and the mortgage market has remained strong. However, new management concerns, including staffing levels and turnover, impact of disrupters like those being seen in the fintech space, and challenges brought on by historically low investment yields have proven to be cumbersome. Yet credit unions have thrived during 2021, and the state of the industry is strong.

State of the unions

Positive outlooks and better-than-expected economic data through 2021 have supported high asset prices; however, the ultimate extent and duration of the pandemic remain one of the more significant risks in the financial system. Despite the pandemic's role in the risk landscape, persistent inflation and monetary tightening are being identified by banks more frequently when looking for risks associated with the next 12–18 months. (Source: FDIC)

Strategic focuses

As credit union boards have conducted their strategic planning meetings, several themes have emerged, including:

- *Digital strategies and evaluation of ROI.*
- *Plans to reallocate internal resources when the record-setting mortgage market cools down.*
- *Investing in business intelligence (BI) and data analytics departments and the development of data governance policies.*
- *M&A strategies.*
- *Re-forecasting budgets with significant increased compensation and facility line items:*
    - *The evaluation of business disrupters or the competitive environment. With several of the large national banks indicating $10 billion-plus technology investments and the ever-increasing emergence of fintech companies targeting traditional credit union projects and services, what will the future bring and how will your credit union adapt?*

While your credit union has likely discussed numerous additional topics, these are a strong indicator of strategic focus areas for institutions this year.

CYBERSECURITY

Three cybersecurity actions every financial institutions should take

Colin Taggart
Principal | Management Consulting
colin.taggart@plantemoran.com

Ben LeClaire
Senior Manager | Management Consulting
ben.leclaire@plantemoran.com

Jennifer Fiebelkorn
Principal | Management Consulting
jennifer.fiebelkorn@plantemoran.com

With cyberthreats on the rise and a steady increase in new regulations, financial institutions need to evaluate their cybersecurity controls and consider taking three key actions to protect their organizations and customer base.

Cyberattacks continue to increase, with hackers seeing potential for profit in essentially any industry. Financial institutions continue to remain a common target, as attackers focus on both an organization and its customer base to potentially wire funds out of the country or hold sensitive data ransom. At the same time, financial institutions continue to expand their technology footprint, requiring increased oversight on security across a wider range of devices, vendors, and cloud platforms.

THE STATE OF CYBERSECURITY

Countless companies in various industries have recently received front-page news coverage for cybersecurity concerns, and the attack trends are continuing to grow. As the threat landscape continues to evolve, it's helpful to look back at how the environment has changed in recent years.

Historically, most organizations had many layers of secure controls in place — such as their trained people, formal processes, and strong technology controls. While some organizations used different tactics than others, the general concept stood that financial institutions had clearly put multiple layers in place to protect the internal environment from external threats.

A few short months into 2020, many companies sent employees to work from home for the first time due to the COVID-19 pandemic. Some organizations had planned ahead (or were fortunate to have recent laptop orders) and could shift quickly to the remote environment. Other organizations had to rush in new VPN setups, roll out new web-accessible applications, or have employees work from home on their personal devices. These projects typically take months of effort in a normal year.

Unsurprisingly, security precautions weren't always taken in these rushed efforts. Similarly, many of these work-from-home options were never anticipated as part of financial institution culture and operations, with gaps in training and procedures now relying on teams making decisions on the fly.

For projects and remote connections implemented over the past year, vulnerabilities still remain. As staff return to offices, personal devices present an emerging risk of transmitting viruses to the secure internal networks. Meanwhile, attackers continue to increase their profits as they send phishing emails tricking employees into clicking links. In addition, the Federal Financial Institutions Examinations Council (FFIEC), Federal Trade Commission (FTC), and third-party vendors continue to raise expectations for security requirements. While these expectations assist with guidance on controls to reduce risk of attacks, the risk of noncompliance with regulatory and vendor contract requirements continues to rise as well.

CURRENT THREATS FACING FINANCIAL INSTITUTIONS

Based on our experience working with financial institutions, we've identified the common trends of critical threats impacting the industry. While there are other additional unique forms of attack, the majority of security incidents we've seen can be tied back to at least one of the following areas:

→ ***Remote security vulnerabilities*** *— With employees working remotely, the line between secure office networks and home networks become heavily blurred. This is particularly concerning when spouses and children also have additional work/school devices that need connecting to the same home wireless network. For employees working from personal devices, their employer may have zero visibility into the security of those devices and may be unaware of any existing viruses stealing data from the device. For financial institutions that recently added remote access, those that didn't add multifactor authentication requirements were exposed to multiple security incidents — with guessed credentials allowing for overseas attackers to easily view emails and other confidential information.*

→ ***Ransomware*** *— Not only are ransomware attacks continuing to rise, but the methods are adapting to respond to companies' efforts to find alternatives to paying out demands. Originally, an attack would focus on encrypting files, requiring companies to pay to unlock unless they had reliable backups to restore from. As more organizations built robust backup controls, attackers have adjusted the threat to focus on publicly releasing data unless ransoms are paid. Attackers will also research organizations to identify appropriate bitcoin ransom amounts to demand and offer a cut of ransom payments to insiders who help provide a foothold into the network.*

→ ***Social engineering*** *— Emails sent to employees tricking them into clicking links and providing credentials are still a main channel for attackers to gain initial footholds into networks. The pandemic provided many opportunities for attackers to mimic expected emails with urgent messages. Additionally, employees working from home can't as easily ask an office neighbor if emails appear suspicious. Our cybersecurity practice has seen a significant rise in click rates during social engineering tests over recent years.*

→ ***Lack of security-dedicated resources*** *— Many financial institutions run lean organizations, relying on IT teammates to also wear information security hats or involve outside vendors to support technology operations. Where internal teams are understaffed, risks increase; in many cases, there's a competition for time and budget to maintain security programs and ongoing technology projects.*

As staff return to offices, personal devices present an emerging risk of transmitting viruses to the secure internal networks. Meanwhile, attackers continue to increase their profits as they send phishing emails tricking employees into clicking links.

RECENT FINANCIAL INSTITUTION REGULATORY UPDATES

Even more frequently than previous years, regulators have continued to update cybersecurity guidance in 2021. Key updates include the following:

- ***January:*** *The Federal Reserve implemented a Security and Resiliency Assurance Program. As part of this new program, institutions and service providers must conduct an assessment of their compliance with the Federal Reserve Banks' FedLine security requirements and submit an attestation that they have completed.*
- ***June:*** *The FFIEC released the Architecture, Infrastructure and Operations IT Exam Handbook, which included an increased focus on data governance, similar topics as the 2019 BCM guidance such as board involvement and system resilience, and new technologies such as remote access.*
- ***July:*** *The FFIEC issued Guidance on Authentication and Access to Financial Institution Services and Systems, with special emphasis on layered security and focus on multifactor authentication options.*
- ***November:*** *The FTC issued a final rule clarifying its data security requirements for certain covered financial institutions, amending the Safeguards Rule originally issued in 2002 under the Gramm-Leach-Bliley Act.*
- ***November:*** *The Office of the Comptroller of the Currency announced a final rule requiring banks to notify their primary federal regulator of any significant computer-security incident as soon as possible and no later than 36 hours after it's determined that a cyber incident has occurred.*

Additionally, the Federal Reserve Banks released an Operating Circular in late 2020, which included expectations for "Security and Resiliency Assurance Program" attestations. With the increase in banks crossing financial thresholds that require additional information security control implementation and auditing, cybersecurity insurance providers have continued to increase requirements before offering insurance coverage. Whether requirements are directly being issued by your regulating entity or not, these various updates are all increasing expectations for financial institution security levels.

ACTIONS TO SECURE YOUR FINANCIAL INSTITUTION

Especially with the volume of changes over recent years, now is the time to reassess your security environment. Ideally, you'll have dozens of complex layered controls in place to consider, and there are a few key items that we typically see as gaps leading to security incidents.

Focusing on these three actions are key initial steps to confirm you're comfortable with the existing setup or to develop a plan to address gaps:

1. ***Enforce password requirements*** *— Strong passwords on all accounts with remote access should be required, as well as multifactor authentication considerations. If software updates aren't under an automated process, a solution may be required. External connections mean the possibility of threat actors attempting to exploit system or application vulnerabilities from afar.*
2. ***Utilize virus scanners and content filters*** *— To defend against ransomware, institutions should ensure virus scanners and content filters are effectively configured on mail servers. Additionally, institutions should employ a data backup and recovery plan for all critical information, and perform and test regular backups to limit the impact of data or system loss and to expedite the recovery process. Note: Network-connected backups can also be affected by ransomware, so critical backups should be isolated from the network for optimal protection.*
3. ***Implement contact training and testing*** *— In instances of social engineering threats, attackers often use compelling stories or arguments to gain entry, whether electronically or physically. Contact training of staff is key to maintain an environment of mindfulness against this sort of activity. Testing should be designed to analyze the effectiveness of contact training, as well as chart progression over a period of time.*

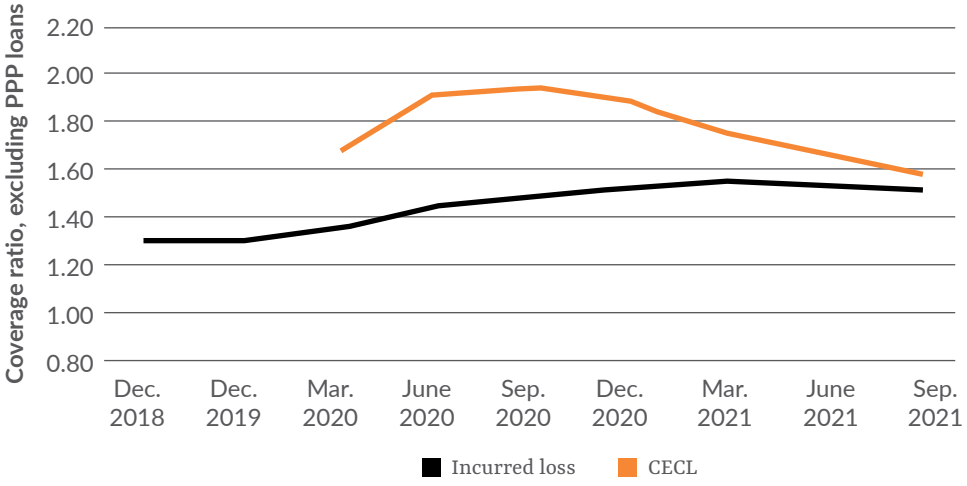
While attackers continue to evolve their approaches and regulators increase expectations, implementing these key controls and proactively planning to strengthen your cybersecurity safeguards can help protect your financial institution. If you have any questions on cybersecurity best practices, please feel free to contact us.

CECL

Where we've been and where we're heading

Based on lessons learned from financial institutions that have already adopted CECL, we've identified two focus areas for institutions yet to adopt, as well as additional and ongoing considerations for all institutions.

As we reflect on the experience of the first 350 institutions to adopt the current expected credit losses (CECL) standard and prepare for the remaining 10,000 institutions to adopt over the coming years, it appears CECL may be achieving the results it was designed for. While it's difficult to distinguish the impact of CECL adoption from that of the pandemic, it appears the standard has allowed institutions to be more responsive to ongoing uncertainty than was common under the incurred loss method.



As we've worked with institutions that have adopted the standard and others that are working toward adoption, we've identified two areas your institution should consider focusing on.

Ryan Abdoo
Partner | Assurance
ryan.abdoo@plantemoran.com

Kate Krones
Senior Manager | Assurance
kate.krones@plantemoran.com

It appears the standard has allowed institutions to be more responsive to ongoing uncertainty than was common under the incurred loss method.

Understanding your model

We've seen institutions design models to estimate credit losses where the resulting reserve conceptually didn't make sense, even though the individual decisions made in developing the model were well supported. This could be the result of not understanding how the model works or certain assumptions having unexpected impacts. To combat this, we suggest taking a moment to assess your model and results from a high level and qualitatively evaluate what you're seeing. Do you have minimal loss history and yet, with almost no adjustments to that history, are projecting a large reserve? Are you expecting an improvement in the economic environment over the next year, but your model is using loss rates that exceed the historical average? The results of these reflections, at a minimum, support the effective challenge of the model and could even lead to some significant adjustments to how you approach establishing a reserve.

Establishing model documentation

Estimating expected credit losses under CECL inherently requires a significant amount of judgment — judgment that will need to be explained to stakeholders such as management and regulators throughout the use of your CECL model. Because of this, we can't stress the importance of establishing and maintaining clear and thorough documentation of decisions made during the development and ongoing operation of the model. While many vendors provide white papers and other technical discussions of the theories underlying third-party models, this documentation should be supplemented with a discussion of how management is applying the model and the related decisions, assumptions, and limitations.

As each institution is in a different stage of addressing the new standard, we've outlined additional considerations for both those who have already adopted and those yet to adopt on the following page.

For institutions yet to adopt:

Most institutions yet to adopt this standard are working toward implementation of a CECL model on Jan. 1, 2023. Below are some key considerations to build into your timeline as you plan for adoption:

- ***Data evaluation:*** *Data availability has been a key consideration in selection of a methodology and/or model. Understanding the data available and trends in your historical loss rates is a good first step for CECL adoption.*
- ***Model selection:*** *The first major decision in selecting a model is determining whether your institution will use an in-house model (often based in Excel) or one developed by a third-party vendor. This decision is often based on an evaluation of the complexity of the institution's loan portfolio, relationships with existing vendors, and level of ongoing effort to maintain an in-house model vs. third-party model. The next decision is which method/model to use and should be based on a thorough understanding of the various options being considered. Again, depth and robustness of data available will likely play a key role in this consideration.*
- ***Parallel runs:*** *Institutions benefit from the opportunity to analyze how their CECL model responds to changes overtime by running the CECL model in parallel with the incurred loss model for a few quarters prior to implementation. Not only does this provide an opportunity to work out process and model issues ahead of adoption, but many institutions we've worked with have found that it helps them better understand their model and provides an opportunity to adjust, if needed, prior to implementation.*
- ***Model validation:*** *Based on the size and complexity of your institution, a model validation prior to implementation may be expected by management, regulators, and/or other stakeholders. We've observed this process to take about three months to complete, and you may want to schedule this to allow for adjustments to the model and additional parallel runs prior to implementation of the model.*

For institutions that have already adopted:

Due to the complex nature of many of the models and methods used to estimate credit losses and the importance of this estimate to your institution, many institutions are realizing that the effort to implement this new standard doesn't stop at the adoption date. As outlined by the regulators, management has a responsibility to perform ongoing monitoring and continue effective challenges of the model and key assumptions throughout the life of the model.

Several important aspects of ongoing monitoring are outlined below. A process to address each consideration should be established and executed on a frequency commensurate with the complexity of the institution and the model.

- *Performing sensitivity analysis to identity key assumptions and verify that the model's response to changes in those assumptions aligns with expectations*
- *Establishing a framework for effective challenge of changes to key assumptions, once identified*
- *Considering how known limitations, overlays, or overrides in your model (for instance, using a floor loss rate in instances where a segment has limited loss history) impact the output of your model at each measurement date*
- *Completing a model validation in accordance with your institution's model risk management program and when significant changes are made to the model*
- *Assessing whether inputs continue to be accurate and consistent with the model's purpose and design*
- *Monitoring the effectiveness of third-party models, including review of SOC-1 reports*
- *Establishing a plan to complete benchmarking and/or outcomes analysis to evaluate the performance of the model*

CREDIT RISK

Effective credit risk monitoring in the post-pandemic economy

John McKay
Senior Manager | Assurance
john.mckay@plantemoran.com

Kevin Garcia
Senior Manager | Assurance
kevin.garcia@plantemoran.com

As COVID-19 continues to affect individuals, communities, and global economies, financial institutions must continually adapt their credit risk monitoring strategies to effectively identify as quickly as possible those loans that have increased in risk. These strategies can help.

The COVID-19 pandemic has forced individuals and businesses to continually adapt to a "next normal," and financial institutions are no exception. While credit risk in the banking industry has, for the most part, remained surprisingly stable throughout this volatile time, the pandemic has driven significant changes in the way financial institutions evaluate credit risk and monitor for signs of deterioration in their existing loan portfolios.

Loan approval is just the beginning of credit risk monitoring

Prior to COVID-19, most financial institutions could reliably determine how they would monitor a loan's performance and assess changes in the borrower's risk profile at the time that they approved the loan. Lenders could use the information gained from the application process to determine what tests could effectively monitor the loan and how frequently to apply them. Tried and true methods could range from analysis of tax returns and financial statements on an annual basis for low-risk loans to more frequent and thorough tools such as covenant compliance checks, evaluation of borrowing base certificates, or the preparation of quarterly or even monthly financial statements. Smaller or less risky loans may be handled on an exception basis only, requiring action only when adverse information is received, such as notification of a judgment, lien, or low credit agency score.

The pandemic has driven home to lenders just how quickly the quality of a loan can deteriorate and how ineffective some of the common tools can be at identifying changes in risk. In addition to the standard reporting requirements that community lending institutions have relied on to monitor the ongoing risk associated with a loan, the following indicators have come to the forefront during the pandemic as helpful early warning signs of potential problems:

- *Rent rolls that provide information on tenants and rents in commercial property can be extremely helpful in assessing the ongoing repayment capacity of the borrowers. They can be particularly useful during the first quarter of the year as a proxy for annual tax return reporting, which is frequently delayed by extensions of the filing date.*
- *Verification of liquidity for borrowers or guarantors where this is considered a significant factor in the underwriting decision.*
- *Use of Smith Travel Research, or "STR," reports for hotel/motel borrowers in order to monitor trends in occupancy, average daily rates, and competitive market position.*
- *Site inspections to verify property condition and occupancy. This would also help detect any potential deferred maintenance and needed capital expenditures.*
- *Field audits on accounts receivable and inventory for borrowing base lines of credit.*

Communication is key

In light of the ongoing macroeconomic pandemic-driven challenges affecting commercial and agricultural enterprises, it's critical for lenders to combine continued credit risk diligence with enhanced borrower communications. Financial institutions can get a much better understanding of changing risk profiles when they talk to borrowers on topics like:

- *Constraints on production or service delivery due to supply chain disruptions, such as a lack of raw materials, component parts, or labor.*
- *Unexpected weather events such as hurricanes, floods, or wildfires that affect industrial output.*
- *Inflation pressures affecting costs of production and the (in)ability to pass these increased costs on to end consumers.*
- *Crop insurance for agricultural production.*

...it's critical for lenders to combine continued credit risk diligence with enhanced borrower communications.

...if a large customer of a borrower is affected by a natural disaster or a COVID-19 outbreak, that customer may be unable to purchase products as previously agreed.

It's also important to remember that even when these challenges don't apply directly to a specific borrower, they can still have an indirect impact on the supply chain or customer base that a borrower counts on. For instance, if a large customer of a borrower is affected by a natural disaster or a COVID-19 outbreak, that customer may be unable to purchase products as previously agreed.

Don't overlook the basics

Lastly, it's important for financial institutions to remember the following monitoring items that may have been put on the back burner while they were addressing the more immediate risks brought about by the pandemic:

- *Succession planning for small business or family-owned enterprises where management is concentrated in one or among a few key personnel.*
- *Tax implications that could arise from the Build Back Better Act or other future legislation.*

These basic components of credit risk haven't disappeared just because businesses have been struggling with more immediate day-to-day challenges of the pandemic.

Without a doubt, the pandemic has touched just about every aspect of our clients' business operations, and the lending area is no exception. It's important that your credit risk monitoring process rely on both time-tested and newly relevant tactics to help your credit management team remain vigilant in the pandemic landscape.

THIRD-PARTY RELATIONSHIPS:

Due diligence guidance for community financial institutions engaging fintechs

New federal guidance has clarified steps that community financial institutions should take when contracting with a financial technology service provider. Institutions that rely on fintechs, and those that are considering new relationships, should take time to understand the expectations.

Today's community financial institutions are seeing more opportunities than ever to enter into relationships with a new generation of financial technology (fintech) companies, including those that offer robotic process automation solutions. Community financial institutions are no strangers to engaging technology companies that assist with various business needs such as core systems and IT infrastructure, but these next-generation fintech partnership opportunities present new risks because the products and services they're offering are new to the marketplace.

Until recently, the regulatory guidance governing third-party risk management expectations for financial institutions has been spread across several different federal agencies. The expectations could vary depending on whether the institution was regulated by the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (FRB), or the Federal Deposit Insurance Corporation (FDIC). This year, the agencies released proposed interagency guidance on risk management for financial institutions entering into third-party relationships, followed shortly after by a guide for community banks that need to conduct due diligence on fintechs. Community financial institutions need to understand this recent guidance and take action to ensure that their third-party risk management programs properly address the relevant risks in fintech relationships.

Brad Birkholz
Senior Manager | Management Consulting
brad.birkholz@plantemoran.com

James Siegel
Manager | Management Consulting
james.siegel@plantemoran.com

A new type of third-party relationship

Partnering with a fintech can be a different risk management experience than partnering with other IT providers. Many community financial institutions have developed third-party risk management processes for their relationships with traditional technology partners — established tech companies like core processing providers FiServ and Jack Henry. These traditional technology partners have typically provided what can be thought of as "standard" IT solutions focused on basic day-to-day "back-office" functions like processing transactions. They usually offer these fundamental services to institutions for less than it would cost the institution to keep the process in house.

Fintech relationships are often (although not always) customer-facing partnerships. They enable community financial institutions to provide a new product or service, access a new customer base, or enhance efficiencies. Financial institutions can't necessarily depend on their technology partners to educate them on the process of partnering with a fintech. These companies are nimble organizations that can change dramatically in short spans of time. As fintechs race to get their products to market ahead of their competition or launch a new version with the latest enhancements, compliance with federal banking regulations probably won't be their top priority. Their culture and business processes may vary greatly from the community financial institutions with whom they partner and from the traditional technology companies that community financial institutions are used to working with.

New guidance to manage these new relationships

In response to the rise of this new type of relationship between community financial institutions and fintech companies, the federal regulatory agencies that oversee America's financial institutions issued proposed interagency guidance on managing risk in third-party relationships. That regulatory language was followed shortly thereafter by a guide focused specifically on helping community financial institutions understand how to conduct due diligence on fintechs under the new guidance. The guide offers relevant considerations, potential sources of information, and helpful examples on the following six key due diligence topics:

- *Business experience & qualifications*
- *Financial condition*
- *Legal & regulatory compliance*
- *Risk management & controls*
- *Information security*
- *Operational resilience*

This action by regulators should streamline the third-party due diligence expectations for all financial institutions. The guide should help community financial institutions understand how their processes may need to be modified in order to perform due diligence on their relationships with fintech companies.

Two types of community financial institutions

At this point, there are two types of community financial institutions in the United States; those that have relationships with third-party fintech companies and those that are going to have relationships with third-party fintech companies. For those that have existing contracts, this guidance serves as a wake-up call that the third-party risk management they've used in the past for relationships with traditional technology partners needs to be reviewed to make sure that they're properly vetting fintech providers. For those that don't yet have relationships with fintech companies, the guide highlights six key due diligence areas in which their third-party risk management process should be reviewed and possibly enhanced before entering into agreements with these service providers.

For many community financial institutions that have been waiting for this guidance in order to start considering relationships with fintechs, the availability of these new expectations could be just the push needed to get them into the market. Still, many community financial institutions aren't well versed in this relatively new guidance and the potential impact it could have on their third-party risk management programs.

Community financial institutions need to read and understand this new joint regulatory guidance, and many will need to update their third-party risk management programs to specifically address fintechs and the risks they present. Those that already have fintech relationships in place will need to determine how this guidance affects their existing relationships and take additional steps as necessary to address any gaps.

We can help with this process, either by performing third-party compliance reviews of potential fintech companies or reviewing a financial institution's third-party risk management processes for compliance with the new expectations. If you have any questions about the new guidance, please contact us.

Fintech relationships are often (although not always) customer-facing partnerships.

FDICIA

FDICIA ROADMAP:

Early planning is key to a successful adoption

Ryan Abdoo
Partner | Assurance
ryan.abdoo@plantemoran.com

Joe Vloedman
Principal | Assurance
joe.vloedman@plantemoran.com

Kristin Golab:
Senior Manager | Assurance
kristin.golab@plantemoran.com

Banks approaching FDICIA requirement thresholds of $500 million and $1 billion in assets need to keep planning top of mind. Preparation is key to a smooth FDICIA adoption, and developing your roadmap early is pivotal to your success.

Since the beginning of the pandemic in March 2020, bank assets have consistently and significantly increased. The increase has triggered additional regulatory requirements at many community banks. The Federal Deposit Insurance Corporation Improvement Act (FDICIA) sets the following two asset-size thresholds for additional compliance requirements:

- *The first set of additional requirements go into effect when a bank charter reaches assets of $500 million or more as of the first date of its fiscal year.*
- *The second set of additional compliance requirements apply once the bank charter reaches assets of $1 billion or more.*

Preparing for the increased compliance requirements is a significant undertaking and early planning is key, especially for the requirements that come along with the $1 billion mark.

New requirements at $500 million

Once a bank exceeds the $500 million mark as of the first day of its fiscal year, it will need to comply with the following three new requirements:

- *First, bank management must prepare a complete set of comparative financial statements with the initial filing to the Federal Deposit Insurance Corporation (FDIC).*
- *Second, management-prepared financial statements must be audited by an auditor that's independent in accordance with the stricter provisions set forth by both the Securities and Exchange Commission (SEC) and Public Company Accounting Oversight Board (PCAOB), regardless of whether the bank is an SEC registrant.*
- *Lastly, the bank will need to establish an audit committee consisting primarily of outside directors.*

It's important to start planning at least a year in advance of crossing this threshold to ensure that the bank's financial statement auditor meets the stricter independence rules, that the bank can develop a plan to prepare its own complete set of financial statements, and that the bank has the time to locate and recruit the right outside directors.

Crossing the $1 billion threshold

Reaching $1 billion in assets represents another critical milestone for any bank. Crossing this threshold adds to the requirements discussed above and is a much larger undertaking. Most notably, when the bank crosses this threshold, the financial statement auditor must be engaged to provide an opinion on the design and operating effectiveness of internal controls over financial reporting. Essentially, think Sarbanes-Oxley but for all banks, even if not registered with the SEC.

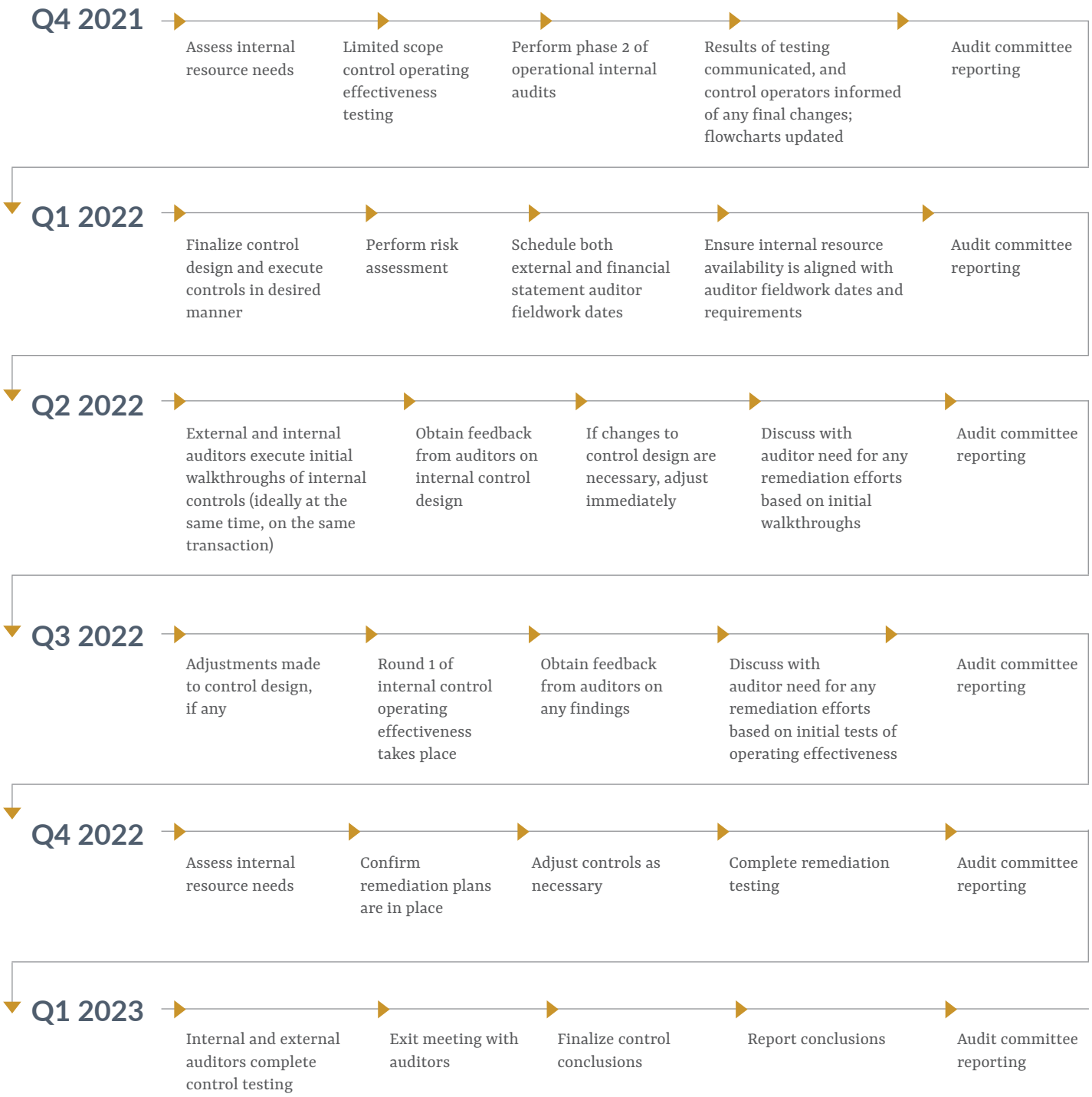
The key to complying with the new requirement at the $1 billion milestone is the early development of a roadmap that ensures a smooth adoption. The bank's goal should be to have internal controls operating as designed beginning on the first day of the fiscal year in which this milestone applies. Board members and management that start late and identify modifications to the design and operation of internal controls midyear often find themselves facing resource constraints and related costs that could have been avoided. The roadmaps on the following pages are designed to assist banks and their audit committees by describing some best practices they can use in evaluating the status of their internal controls implementation.

With the expiration of the FDICIA relief provided by the regulators, many banks will be implementing one of these FDICIA thresholds. A proactive approach with constant monitoring and communication between all parties is a must. To assist with the oversight, we recommend developing a roadmap with milestones to monitor and stay on track for a successful adoption.

We recommend developing a roadmap with milestones to monitor and stay on track for a successful adoption.

Roadmap #1: For banks where the more significant requirements of the $1 billion threshold will first apply for their calendar year ending Dec. 31, 2023, based on the Jan. 1, 2023 measurement date.

Roadmap#2: For banks where the requirements of the $1 billion threshold will first apply for their calendar year ending Dec. 31, 2022, based on the Jan. 1, 2022 measurement date.



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
- Cybersecurity
- ITGC & GLBA assessment
- Network security
- Social engineering
- Operations consulting & improvement
- Human resource effectiveness & employee benefits consulting
- 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

225+
community bank clients

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

Industry involvement

Participation in national and state associations for bankers, including:

- 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
- 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

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

Practice profile

20 partners

200 industry professionals

50+ years serving financial institutions

OUR LEADERS

Brian Franey
CPA | Audit partner
brian.franey@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
Rob leads Plante Moran's financial institutions practice.

Kevin Conte
CPA | Audit partner
kevin.conte@plantemoran.com

Jeannette Contreraz
CPA | Tax partner
jeannette.contreraz@plantemoran.com

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, FIRM | Audit partner
sherrie.krowczyk-mendoza@plantemoran.com

Kyle Manny
CPA, CGMA | Audit partner
kyle.manny@plantemoran.com

Joe Oleksak
CISSP, CRISC, QSA | 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 Petree
CPA, CISA, CISSP, CFE, QSA | Consulting partner
scott.petree@plantemoran.com

Scott Phillips
CPA, CIA | 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
CICA | 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

Colleen Wellman
CPA | Audit partner
colleen.m.wellman@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 lauren.heimler@plantemoran.com.

Stay in the know: **plantemoran.com/subscribe**

plantemoran.com

FS.GB01.012022