P&G Banking ADVISOR

Fall 2019

MAKING THE TRANSITION TO FDICIA REPORTING: GET AN EARLY START

ARE YOU PREPARED?
5 common cyber threats to the banking industry

KNOW THE RISKS OF THE SECONDARY MARKET MORTGAGE BUSINESS

BANK WIRE

P&G Associates

www.pandgassociates.com 877.651.1700

MAKING THE TRANSITION TO FDICIA REPORTING: GET AN EARLY START

The Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) was designed to strengthen the FDIC and improve the safety and soundness of financial institutions. It imposes stricter auditing, reporting and governance obligations on institutions as their assets cross the $500 million and $1 billion marks.

As your bank grows — either organically or through mergers and acquisitions — it's important to anticipate when it will reach these thresholds and begin to prepare well in advance. Starting early helps you ensure a smooth transition and gives you an opportunity to do a "dry run" of new internal controls and procedures. That way, you can remedy any deficiencies before you're required to report them to banking regulators.

WHAT'S REQUIRED?

Once your bank reaches $500 million in assets, you'll need to take the following steps:

- Prepare audited comparative annual financial statements and submit them, together with the independent public accountant's report, to the appropriate federal banking agency within 120 days after the end of the fiscal year (90 days for publicly traded banks).
- Comply with the same auditor independence standards that apply to public companies. (See "Is your auditor independent?" on page 3.)
- Submit annual management reports that include a statement on management's responsibility for 1) preparing financial statements, 2) establishing and maintaining an adequate internal control over financial reporting (ICFR) structure, and 3) complying with certain safety and soundness laws and regulations.
- Maintain an audit committee, a majority of whose members are outside directors independent of management.

At $1 billion in assets, in addition to the above, your bank must do the following:

- Submit expanded management reports, including an evaluation of the effectiveness of your bank's ICFR as of the end of the fiscal year, based on a recognized framework. Most banks use the *Internal Control — Integrated Framework* developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).
- Submit an independent auditor's attestation report on the effectiveness of ICFR as of the end of the fiscal year.
- Maintain an audit committee, *all* of whose members are outside directors independent of management.

Many of these requirements will be time and resource intensive — particularly the enhanced documentation and testing necessary to evaluate and attest to the effectiveness of ICFR.

HOW SHOULD YOU PREPARE?

When your bank reaches the above thresholds, the new requirements take effect at the beginning of the next fiscal year. But if you wait until then, you may have to implement them quickly. This may create stress, increase your costs and jeopardize your ability to transition effectively to the new financial reporting environment. A better approach is to track your growth closely, estimate when you'll reach the threshold and begin preparations well in advance — ideally 18 to 24 months before the new requirements take effect.

As you develop your plan for crossing the $500 million threshold, here are some key issues to consider. If you don't currently prepare audited financial statements, consider at least a balance sheet audit for the year before you become subject to FDICIA requirements. Your auditor's report will discuss any material weaknesses or significant deficiencies in your ICFR revealed during the audit. Thus, this step allows you to identify and remedy problems before you're required to submit the report to federal regulators.

In addition, review the services you receive from your accountants to identify potential independence issues that may arise once you cross the threshold. If you anticipate conflicts, start planning for separate firms to provide audit services and prohibited nonaudit services. Keep in mind that your auditor won't be permitted to draft your financial statements, so management will need to assume more responsibility for financial statement preparation and review. Be sure that you have the personnel you need in place — as well as appropriate controls and procedures — by the time the FDICIA requirements take effect.

Finally, review the composition of your board of directors to ensure that you can appoint an audit committee with a majority of independent members. If it's necessary to add directors, leave ample time to conduct a thorough search.

IS YOUR AUDITOR INDEPENDENT?

FDICIA-covered banks are subject to the same auditor independence requirements as public companies. Among other things, that means your financial statement auditor must avoid specific conflicts of interest and prohibited financial relationships with the bank, rotate audit partners at least every five years, and refrain from providing prohibited nonaudit services to the bank.

Prohibited services include:

- Bookkeeping,
- Financial statement preparation,
- Valuation,
- Outsourced internal audits (including loan reviews),
- Tax return preparation for individuals in a financial reporting oversight role (or their family members), and
- Financial information systems design and implementation.

WHAT'S YOUR PLAN?

Advance planning is even more critical as you approach the $1 billion threshold. In addition to the steps outlined here, you'll need time to incorporate a recognized ICFR framework and appoint a fully independent audit committee. The former may require you to modify your ICFR structure and procedures and to develop a process for evaluating their effectiveness.

If you expect your bank to grow large enough to trigger FDICIA requirements, start to prepare as early as possible. By developing a detailed implementation plan and beginning to phase in changes before you have to, you can minimize disruptions and avoid issues after the requirements take effect. ■

ARE YOU PREPARED?

5 common cyber threats to the banking industry

It's easy to see why cybersecurity is one of the most critical issues businesses face today. All you need to do is pick up a newspaper or turn on the TV to learn about the latest data breaches and other cyberattacks. And it's no surprise that the banking industry is among those most affected by these attacks.

GET TO KNOW THE THREATS

Recognizing the problem and determining what to do about it, of course, are different things — and many bank executives aren't sure where to start. A good first step is to become familiar with some of the most common cyber threats. Then you can conduct a risk assessment to identify and quantify your institution's specific vulnerabilities and develop a plan for addressing these threats.

> BANKS CAN MITIGATE THE IMPACT OF RANSOMWARE ATTACKS BY DEVELOPING ROBUST BUSINESS CONTINUITY PLANS AND INCIDENT RESPONSE PLANS.

Here are five of the most common cyberattacks used against banks:

1. Malware. These malicious software programs or codes are introduced into the bank's system via email attachments, removable media (such as flash drives) or downloads from phony websites. Not only can malware compromise the confidentiality and integrity of sensitive customer data — it also can destroy data or disrupt your systems. Techniques for avoiding malware include training employees to recognize potential problems, requiring email attachments to

be scanned, placing restrictions on use of removable media and ensuring that systems are updated with the latest security patches.

2. Phishing and business email fraud. Phishing involves attackers who create and send seemingly legitimate emails to bank personnel or customers to trick them into revealing login credentials or other sensitive information or to transfer funds. An increasingly common technique is to impersonate a client's CEO or other executive and to instruct an employee to wire funds to the attacker's account. These attacks can be minimized through training and additional controls, such as requiring confirmation of wire transfer details by phone.

3. Ransomware. This is a form of malware that encrypts files in your system and demands a ransom in exchange for the encryption key that unlocks them. In addition to general safeguards against malware, banks can mitigate the impact of ransomware attacks by developing robust business continuity plans and incident response plans.

4. Denial of service. In a distributed denial-of-service (DDoS) attack, the attacker uses bots or other tools to

flood the bank's servers with Internet traffic, slowing or shutting down traffic from legitimate users. DDoS attacks may be politically motivated — or they may be used as a diversion to conceal another type of attack. To mitigate the risk, banks should monitor website traffic, develop strong incident response plans and consider using third-party service providers to manage Internet traffic.

5. Watering hole. In this technique, which has been used to target banks in recent years, an attacker identifies less secure websites visited regularly by bank employees, such as a vendor's website — or even a shopping or online food delivery service. The attacker then infects that site with malware. The hope is that a bank employee's computer will become infected, thus compromising the bank's systems. Techniques for defending against these attacks include monitoring website traffic, inspecting sites visited by employees for malware (and blocking infected sites), keeping systems up to date and ensuring that employees use current, properly configured browsers.

UNDERSTAND THAT CYBER THREATS EVOLVE

These are just a few of the many cyber threats against banks today. As you can see from the variety of techniques used, cyber attacks may be designed to steal money or information or disrupt bank operations. They may target the bank itself, its customers or its service providers.

And attackers don't just focus on technological vulnerabilities. They also use social engineering techniques to trick people into divulging confidential information or providing attackers with access to bank systems.

ASSESS YOUR RISK

The key to combating cyber threats is to conduct a comprehensive risk assessment that identifies your bank's potential access points and vulnerabilities and quantifies the potential cost of a breach. Armed with that information, you can develop a plan for avoiding or mitigating these risks. ■

KNOW THE RISKS OF THE SECONDARY MARKET MORTGAGE BUSINESS

In an increasingly competitive environment, many community banks are seeking to improve their bottom line with new strategies. One approach they've been turning to more frequently in the past few years is selling the mortgage loans they've originated to the secondary market. But banks that don't have a good grasp of the risks and rewards of this approach may end up losing out.

THE HISTORY

Traditionally, community banks that participated in the secondary market were brokers, originating mortgages closed on behalf of larger financial institutions. In 2013, the Consumer Financial Protection Bureau (CFPB) finalized new loan originator compensation rules, which substantially limited the fees a broker could earn.

Since then, many community banks, in an effort to enhance noninterest income, have begun originating mortgages on their own behalf and then selling them to secondary market investors.

EXPOSURE TO RISK

Community banks that move away from the broker role and originate their own loans increase their risk exposure. For one thing, they become subject to CFPB

rules, including the Ability-to-Repay (ATR) and Qualified Mortgage (QM) rules. Even after selling a loan to the secondary market, a bank remains liable under these rules and may be required to buy back the loan years later if it's determined that it failed to properly evaluate the borrower's ability to repay or to meet qualified mortgage standards.

To mitigate these risks, it's important for banks to develop or update underwriting policies, procedures and internal controls to ensure compliance with the ATR and QM rules. It's also critical for banks to have loan officers and other personnel in place with the skill and training necessary to implement the rules.

In addition, there's a risk that contracts to sell mortgages to the secondary market will have a negative effect on a bank's regulatory capital. Often, these contracts contain credit-enhancing representations and warranties (CERWs), under which the seller assumes some of the risk of default or nonperformance. Generally, these exposures must be reported and risk-weighted (using one of several approaches) on a bank's call reports, which can increase the amount of capital or reserves the bank is required to maintain.

THE BASEL III CAPITAL RULES

The Basel III capital rules provide a safe harbor that exempts certain representations and warranties from the risk-based capital rules. For example, CERWs don't include:

- Early default clauses and similar warranties in connection with qualifying one- to four-family residential first mortgages that permit a buyer to return a loan (or obtain a premium refund) in the event of default for a period not to exceed 120 days from the original sale,
- Premium refund clauses in connection with certain government-guaranteed loans, and
- Warranties that permit a buyer to return a loan in cases of misrepresentation, fraud or incomplete documentation.

If, however, a loan sale agreement contains an early default period that exceeds 120 days, the bank must risk-weight the warranty until it expires.

THE DEVIL IS IN THE DETAILS

When entering into loan sale agreements, it's important for community banks to pay close attention to the details — including all representations and warranties. This will help them determine the effect these terms will have on regulatory capital. If your bank decides to go beyond a broker role and take steps to originate its own secondary market mortgages, you'll need to weigh the risks along with the rewards. ■

BANK WIRE

FASB PROPOSAL DELAYS CECL, LEASE ACCOUNTING CHANGES

A recent proposal by the Financial Accounting Standards Board (FASB) provides some breathing room for community banks struggling to implement the current expected credit losses (CECL) model and the new lease accounting standard. Currently, for privately held, calendar-year banks, CECL is scheduled to take effect in 2021 and the new lease standard is scheduled to take effect in 2020. FASB's proposal would delay these effective dates to 2023 for CECL and 2021 for lease accounting. The FASB is releasing its proposal for public comment, but is expected to finalize the changes by the end of the year. ■

CRA REFORM

The Community Reinvestment Act (CRA) is designed to encourage banks to help meet their communities' credit needs. Federal banking regulators periodically evaluate how banks have served their communities. They consider those evaluations in determining whether to approve bank mergers, branch openings and other expansions.

In connection with efforts to reform the CRA, the Federal Reserve recently issued a report entitled *Perspectives from Main Street: Stakeholder Feedback on Modernizing the Community Reinvestment Act*. Participants' suggestions included expanding assessment areas beyond current geographic boundaries; updating asset thresholds to determine whether a bank is small, intermediate or large; improving and clarifying the metrics used to evaluate performance; and clarifying and expanding what qualifies as an eligible community development activity.

The federal banking agencies are expected to issue proposed regulations on CRA reform early next year. ■

CORE LENDING PRINCIPLES FOR HIGH LTV LOANS

Recently, the OCC issued Bulletin 2019-28, which outlines "core lending principles" for higher loan-to-value (LTV) loans. The bulletin expressly rescinds Bulletin 2017-28 —"Mortgage Lending: Risk Management Guidance for Higher-Loan-to-Value Lending Programs in Communities Targeted for Revitalization" — observing that "banks have engaged in responsible, innovative lending strategies that are different from that bulletin's specific program parameters while being consistent with its goals."

The new bulletin encourages banks to refer to the OCC's core lending principles in connection with their community revitalization efforts. The guidance urges banks making higher LTV loans to 1) ensure the loans are consistent with safe and sound banking, treat customers fairly, and comply with applicable laws and regulations; 2) effectively monitor, track and manage loan performance; and 3) underwrite the loans in a manner consistent with *Interagency Guidelines for Real Estate Lending Policies* as well as the bank's own standards for review and approval of exception loans.

The bulletin provides several examples of sound policies and processes specific to higher LTV loans. ■

P&G Associates

P&G Associates ("P&G") has been meeting the specific risk management needs of community banks of all sizes since 1991. As a high quality and affordable alternative to national firms, P&G provides internal audit, regulatory compliance, BSA/AML, information technology and enterprise risk management review services and software. P&G is exclusively dedicated to the banking industry, providing clients with dedicated, focused and hand-held services reflective of a wide range of skills, experience and industry expertise. As a Firm, we have also been proactive in assisting our clients with the designing, implementation and testing of the internal control environment to assist management with the attestation requirement under the Sarbanes-Oxley Act.

P&G's uniqueness is characterized by its experienced staff and partners. Their hands-on involvement on each engagement provides our clients with a wide range of skills, experience and industry expertise. We employ the use of Subject Matter Experts — designated individuals performing audits in their specific field of expertise. The use of such professionals provides a unique value-added approach that is both efficient and productive.

We believe that a significant aspect of our services is our degree of involvement and responsibility to assist management by making suggestions for improvement, keeping them informed of professional developments and by acting as an independent counsel and sounding board on general business matters and new ideas.

We pride ourselves in our ability to provide effective and practical solutions that are commensurate with our clients' needs by emphasizing high-quality personalized service and attention. Our services are truly customized.

For **Solutions** *to your internal audit needs, please contact our service coordinators at (877) 651-1700, or log-on to www.pandgassociates.com to learn more.*

P&G Associates

www.pandgassociates.com

Headquarters:
646 US Highway 18
East Brunswick, NJ 08816

Offices:
New York, NY
Philadelphia, PA
Chicago, IL
Miami, FL