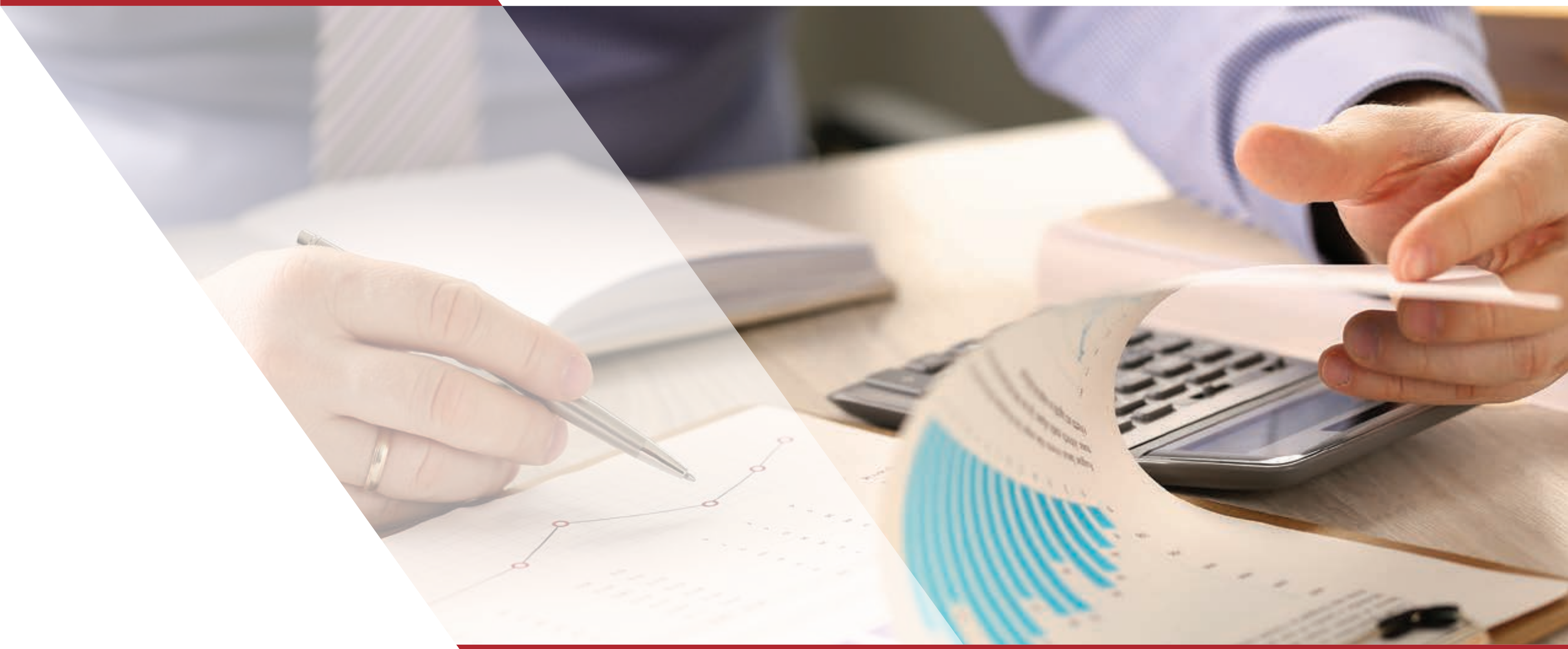
Fall 2020

COMMUNITY BANKING ADVISOR



NOW'S THE TIME TO REVIEW YOUR INTERNAL CONTROLS

HEDGE YOUR BETS
Balance risk vs. reward in asset concentrations

ARE OFF-SITE BANK EXAMINATIONS HERE TO STAY?

BANK WIRE

acxell

www.acxellrms.com 877.651.1700

NOW'S THE TIME TO REVIEW YOUR INTERNAL CONTROLS

The COVID-19 pandemic has had a dramatic impact on the way banks and other organizations do business. Some banks have closed branches — and many are operating with reduced staff or relying more heavily on remote workers. These conditions create internal control challenges. Staff reductions make it more difficult to segregate duties, potentially increasing the bank's risk of fraud and error. It's a good idea for banks to review their internal control policies and procedures and consider strategies for making them more efficient and effective.

MANAGING RISK

Weak or ineffective internal controls can expose the bank to a higher risk of fraud, which can lead to significant losses and even threaten the bank's continued operations. According to the most recent occupational fraud survey by the Association of Certified Fraud Examiners, the top three factors that contribute to fraud are lack of internal controls (32%), lack of management review (18%) and override of existing controls (18%).

Segregation of duties is a key control for banks. Assigning different people responsibility for authorizing transactions, recording transactions and maintaining custody of assets makes it virtually impossible for a single employee to both commit fraud and conceal it. Banks with reduced staff should assess the impact on segregation of duties and consider alternative procedures that can help mitigate the risk. For example, some banks are asking their personnel to open and count cash deposits in front of security cameras, or allowing authorized check signers to approve checks via email if they can't be physically present.

PREVENTING VS. DETECTING

Internal controls generally can be classified as either "preventive" or "detective." *Preventive* controls — such as segregation of duties, preapproval of certain transactions, strong computer passwords and physical control of assets (for example, locks) — head off fraud and errors before they occur. *Detective* controls help spot fraud or errors after the fact. They include management review, surprise cash counts, reconciliations and internal audits.

By definition, detective controls are less effective than preventive controls in mitigating the risk of fraud and errors. They also may be inefficient or impractical, particularly in the current climate of reduced staff and remote workers. So it's important to focus on preventive controls. That's not to say that detective controls should be ignored. The mere possibility of surprise audits, management reviews or other detective measures can also have a strong deterrent effect.

USING APPLICATION CONTROLS

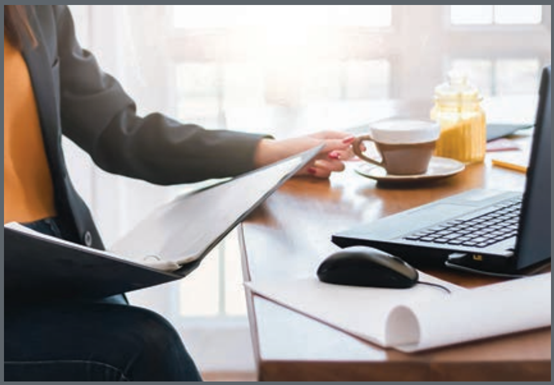
While most banks routinely use sophisticated software programs and platforms, they often fail to fully use preventive application controls that might substantially reduce risk. These controls can be as simple as

CYBERSECURITY TIPS FOR REMOTE WORKERS

Remote work has become a way of life for many banks and other businesses. And while it's a great way to keep workers productive in the current environment, it also introduces new vulnerabilities to hacking and other cybercrime. Here are several tips for making remote work as safe as possible:

Encourage or require employees to avoid unsecured Wi-Fi networks. Employees should use only Wi-Fi networks that are password protected or, ideally, use an encryption key. Better yet, consider requiring employees to use wired connections, which are more secure and also faster. For an additional layer of protection, have remote workers use a virtual private network (VPN) and multifactor authentication to connect and log in to the bank's systems.

Make sure remote employees use bank-provided devices that are properly maintained. Protect your devices with the latest patches and other security features. If use of personal devices is unavoidable, ensure that employees get the most recent updates of all operating systems and applications, turn on firewalls, and run regularly updated antimalware software on their computers.



Discourage remote employees from storing sensitive data on their personal devices. Instead, have them use cloud-based storage or the bank's servers. If they must store data at home, have them use an encrypted external hard drive they can easily bring into the office when needed.

Provide employees with training on how to avoid phishing and other cyberattacks. For example, educate employees on the telltale signs of a malicious email, such as typos, poor grammar or requests for confidential information. Train them to hover over links before clicking to make sure they lead to legitimate websites.

restrictions on the ability of bank employees to access particular functions, or to input or modify specific information. For example, some banks offering online banking allow only customers to change their own account information online. This limits bank employees' ability to make account changes, because they can only do so for those customers who don't use online banking. This approach makes the management review process more efficient by reducing the number of account changes that require review.

Banks should review their systems and identify application controls that can reduce their risks — either by restricting employee access or automating certain processes. The need for management reviews can never be eliminated, but application controls can reduce reliance on such reviews and ensure that they focus on where they can be most effective.

TAKING ADVANTAGE OF THE OPTIONS

These are just a few ways banks can modify their controls or establish new ones that mitigate risk without overburdening their staffs. It's important to review the options on an ongoing basis to ensure all possible steps are being taken to help prevent and reduce fraud. ■

HEDGE YOUR BETS

Balance risk vs. reward in asset concentrations

The mission of most community banks is obvious: to serve their communities. But each community has its own specific economy, often based on just one or two industries, with a smattering of others in the mix. Primarily lending to just one industry, whether it's to farmers, manufacturers or any other group, can throw a community bank's loans out of whack and make it tough to recover if that industry takes a hit. How can you balance risk and reward as you provide lending services to local industries?

MANAGE YOUR ASSET CONCENTRATIONS

Asset concentrations increase a bank's risk by exposing it to significant potential losses. But that doesn't mean that banks should avoid such concentrations at all costs. On the contrary, asset concentrations enable banks to better operate within their communities by taking advantage of local industry expertise and market knowledge. The key to managing asset concentrations is to take a balanced approach that weighs the risks against the benefits — and to implement measures to mitigate those risks.

Here are some best practices banks should consider when addressing asset concentrations:

Review credit risk management policies. Evaluate these policies, keeping in mind that asset concentration risks are felt well beyond the area of concentration. Suppose a bank has a heavy concentration of loans to businesses in a particular industry. A downturn in that industry could not only affect the ability of businesses in the industry to repay their loans, but could also make it harder for individuals who work in the industry to repay their auto loans or mortgages.

So it's critical to consider the impact of asset concentrations on your entire loan portfolio and to implement policies to address the elevated risk. Such policies might include tightening underwriting standards, placing caps on asset concentrations and conducting global cash-flow analyses. You also should invest in stress testing and monitor loans carefully.

ASSET CONCENTRATIONS ENABLE BANKS TO BETTER OPERATE WITHIN THEIR COMMUNITIES BY TAKING ADVANTAGE OF LOCAL INDUSTRY EXPERTISE AND MARKET KNOWLEDGE.

Evaluate capital and reserves. Ensure that your bank's level of capital and reserves is commensurate with its concentration risk. If your bank has a significant concentration of loans in a particular industry, market or loan type, it's important to consider the relationships among these loans when evaluating the sufficiency of your capital and determining an appropriate allowance for loan and lease losses (ALLL).

Take a judicious approach to diversification. An obvious solution to a risky asset concentration is to diversify. But diversification presents its own risks, so it's important to handle the process carefully. For example, a bank with a heavy concentration of loans in one industry or geographic territory might diversify by making loans to businesses in other industries or territories. But doing so would require the bank to venture out of its comfort zone into areas where it might not possess the same level of knowledge and expertise.

Look for ways to diversify *within* a particular industry. For example, a bank with a high concentration of agricultural loans should consider lending to both crop producers, such as corn or soybean farmers, and livestock producers. This can mitigate the bank's risk because economic and other external forces that hurt one industry segment may help the other. A decline in crop prices, for instance, would harm crop producers but it could benefit livestock producers by reducing their feed costs.

Another diversification strategy is to increase the size of your bank's securities portfolio. Doing so instantly shrinks the bank's loan-to-asset ratio. (A high ratio is often a red flag.) But keep in mind that investing in securities poses problems of its own and may divert capital away from the community your bank serves.

KNOWLEDGE IS POWER

Clearly, your community bank operates within the local economy and is dependent on it. So understanding the ins and outs of how local businesses function, within your community and beyond, will give you a leg up — helping your bank thrive by managing your asset concentrations while supporting your community's businesses as they grow and develop. ■

ARE OFF-SITE BANK EXAMINATIONS HERE TO STAY?

During the COVID-19 pandemic, many banking regulators have shifted to an off-site, or remote, examination process. Even before the pandemic, regulators sometimes used off-site examinations during natural disasters or other extraordinary circumstances. And off-site monitoring and electronic document exchange has been a routine part of the examination process in many cases.

Many people believe that off-site examinations — with their obvious efficiencies and other benefits — will become standard operating procedure in the future. While this remains to be seen, the pandemic has put the spotlight on the benefits and challenges associated with this approach.

GET TO KNOW THE FED'S VIEW

In a recent publication, the Federal Reserve discussed its use of off-site examinations under unique circumstances, such as the COVID-19 pandemic. Here are some answers to key questions.

What are the considerations? When determining the appropriateness of off-site exams, examiners consider several factors, including a bank's risk profile, management preferences and technological capabilities — particularly for loan file review.

What are the benefits? Technological advances over the last decade have transformed the bank supervision process, such that much of the work is now done off

site. Off-site examinations offer significant benefits, in terms of convenience and continuity, for banks and examiners alike — particularly under extenuating circumstances that make on-site work impractical or impossible. Although preparing for an off-site examination requires greater coordination, the potential benefits are substantial, including:

- Procedural efficiencies, such as minimizing disruption of bank activities,
- Greater flexibility for the Fed to manage resources, and
- Ability to offer training and mentoring opportunities for newer examiners.

The Fed also observed that, in light of COVID-19, it "adjusted its supervisory approach to focus on monitoring and outreach to help financial institutions … understand the challenges and risks posed by the current environment." The pandemic highlighted the importance of off-site monitoring and examination support.

How can you communicate effectively? Whether an exam is conducted on site or off site, Fed staff must be able to communicate effectively with bank management. On-site visits, when appropriate, remain a valuable practice for fostering an open dialogue between examiners and bank management and building positive working relationships. Communications between a bank and off-site examiners can be challenging because of the lag time between messages. But these problems can be mitigated if both sides act promptly in addressing requested items, scheduling meetings and acknowledging receipt of messages.

What about technology? A key factor in determining whether off-site examinations are feasible is a bank's technological capabilities. Consider loan review, for example. The decision as to whether to perform a loan review off site depends in large part on whether the bank has the technological capabilities and resources to provide electronically imaged loan files in a readable and secure manner. The Fed recognizes that not all banks have the ability or desire to facilitate off-site loan review, and notes that this process "will continue to evolve and be refined over time."

> TECHNOLOGICAL ADVANCES OVER THE LAST DECADE HAVE TRANSFORMED THE BANK SUPERVISION PROCESS, SUCH THAT MUCH OF THE WORK IS NOW DONE OFF SITE.

STAY TUNED

The postpandemic future of off-site examinations remains to be seen. Based on the Fed's quality assurance reviews, it has found that off-site examinations don't materially affect overall outcomes. But the Fed also recognizes that some well-managed banks prefer the relationship-building benefits of on-site examinations — and it plans to honor such requests. ■

BANK WIRE

FFIEC UPDATES BSA/AML EXAMINATION MANUAL

Recently, the Federal Financial Institutions Examination Council (FFIEC) made several significant revisions to its *Bank Secrecy Act / Anti-Money Laundering Examination Manual*. The revisions:

- Add a section on risk-focused BSA/AML supervision, emphasizing the need to tailor examinations to a bank's risk profile,
- Clarify that there's no particular method or format a bank must use for the risk assessment,
- Clarify that risk assessment updates aren't required on a continuous or specified periodic basis — rather, risk assessment updates should align with significant changes in a bank's risk profile, and
- Remind examiners that banks have flexibility in designing their BSA/AML compliance programs — and that minor weaknesses, deficiencies and technical violations alone aren't indicative of an inadequate program. ■

OCC PROPOSES VIRTUAL MEETINGS

The Office of the Comptroller of the Currency (OCC) has proposed an update to its regulations that permits banks to hold in-person meetings — such as director, shareholder and member meetings — using remote communication tools.

Under the agency's interim final rule, remote participants would be deemed present in person for quorum purposes. To take advantage of the new rule, a bank would have to amend its bylaws. Although this change was prompted by the advent of COVID-19, it will be permanent and won't expire when the pandemic emergency has ended. ■

OCC HIGHLIGHTS KEY BANKING RISKS

In June, the OCC released its Spring 2020 *Semiannual Risk Perspective*, reporting key issues facing the federal banking system. It also noted the effects of COVID-19 on the banking industry.

Among other things, the report finds that compliance risk is elevated. This is because of a "combination of altered operations, employees working remotely, and several new federal and state programs designed to support consumers." ■

FFIEC PROVIDES CLOUD COMPUTING GUIDANCE

An increasing number of banks are relying on the cloud to facilitate remote work and other social distancing practices. The cloud offers a variety of benefits, but it also introduces significant risks that need to be considered.

In a recent joint statement, the FFIEC provides some welcome guidance. The FFIEC warns bank management not to assume that effective controls are in place. Rather, management should conduct due diligence and follow sound risk management practices in connection with cloud service provider relationships to verify that they have effective security, operations and resiliency controls. The statement outlines best practices. To see it, visit ffiec.gov and click on "Press Releases," followed by the "April 30, 2020" link. At the bottom of the page that next appears, click on the "Cloud Computing" joint statement at the bottom. ■

acxell ("acxell") has been meeting the specific risk management needs of community banks of all sizes since 1991. As a high quality and affordable alternative to other firms, acxell provides internal audit, regulatory compliance, BSA/AML, information technology, SOX/FDICIA and enterprise risk management review services and software. acxell 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.

acxell'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 risk management needs, please contact our service coordinators at (877) 651-1700, or log-on to www.acxellrms.com to learn more.*

www.acxellrms.com

Headquarters:
646 US Highway 18
East Brunswick, NJ 08816

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