Banking IN THE NINTH

SEPTEMBER 2017

NINTH DISTRICT HIGHLIGHTS

Embracing Change

Christine Gaffney

Effective June 1, I began a new position at the Minneapolis Federal Reserve Bank as the head of Supervision and Regulation. Many of you built a relationship with Ron Feldman during his tenure in this position, and I look forward to doing the same. I had the opportunity to work directly for, and learn from, Ron for nearly 10 years. I intend to use the knowledge and experiences I gained, and I also intend to take the time to listen to key stakeholders, internally and externally, to determine how and where we can collectively benefit from change.

For my inaugural Banking in the Ninth article, I will reflect on change. Change is inevitable, yet it can be challenging because people tend to fear the unknown. As we embark upon this change of leadership in the Supervision and Regulation function, we have a great opportunity to think about what change means, why it is important in the work we do and why we need to be open to embracing the unfamiliar.

Comfort in familiarity

Human nature lends itself to taking comfort in what's familiar. The challenge with this is that our current financial and regulatory environment is filled with unknowns—whether it is regulatory reform, the current political administration or the next greatest risk to the financial system. It is paramount that as financial institution supervisors, we do not rest on the comfort of the variables we know. Rather, we need to be attuned to the changing environment in which we operate and adjust accordingly. To do this, as supervisors, we want to ensure that we are listening to the concerns of the industry. It also means we need to be comfortable with the unfamiliar when we find it is necessary to adjust course. In our organization, we refer to this as "leading in ambiguity." We often emphasize the importance of this with our leaders.

As we embark upon this change of leadership in the Supervision and Regulation function, we have a great opportunity to think about what change means, why it is important in the work we do and why we need to be open to embracing the unfamiliar.

The evolving supervisory process

Those of you who have been in the financial industry for some time are well aware of the changes we've implemented over the years in our supervisory processes. Indeed, this issue of the newsletter provides an update on some of our changes related

continued on page 3

SAFETY & SOUNDNESS UPDATE

Saftey and Soundness Off-Site Work Update

Aaron D. Zabler, Assistant Vice President
Mark Rauzi, Vice President

In the September 2014 issue of Banking in the Ninth, we shared our efforts to conduct more aspects of our examinations off-site (i.e., not at the bank). Three years later, that trend continues as we strengthen and improve the process. Overall, the shift is mutually beneficial, but not without challenges. In this article, we recap the progress made—the benefits and challenges of conducting off-site exams—and we share and solicit feedback on this change.

As technology has surely changed at your institutions, it has, in turn, changed the way we conduct exams. Now that institutions largely maintain their records electronically, and we have built and use systems to manage and

continued on page 3

Updated Interagency Consumer Compliance Rating System

Alex Restrepo, Assistant Examiner

State member banks (SMBs) and other federally regulated banks will now receive consumer compliance ratings based on an updated interagency rating system. The Federal Financial Institutions Examination Council (FFIEC) issued the Uniform Interagency Consumer Compliance Rating System (CC Rating System) in November 2016.[1] The Federal Reserve System is applying the CC Rating System to exams that began on or after March 31, 2017. The updated system better reflects how we currently examine our SMBs, focusing on the SMB's compliance management program and how effectively that program manages the SMB's compliance risk. The updated system also supports comprehensive and consistent evaluation of financial institutions across the federal regulatory agencies and focuses supervisory resources on higher-risk areas. In this article, I discuss the factors that examiners will consider when determining a bank's compliance rating, as well as some ways that banks can use the system to evaluate their own compliance programs.

How examiners will use the CC Rating System

What factors will examiners consider in determining a compliance rating? Banks will continue to receive a consumer compliance examination rating based on a scale of 1 to 5.[2] The rating system includes definitions for three rating categories that consist of qualitative descriptions rather than one definition for each rating. Specifically, examiners will evaluate the following 12 assessment factors, organized under three main categories, to determine the rating:

1. ***Board and Management Oversight***
   - Oversight and Commitment
   - Change Management
   - Comprehension, Identification, and Management of Risk
   - Corrective Action and Self-Identification

2. ***Compliance Program***
   - Policies and Procedures
   - Training
   - Monitoring and/or Audit
   - Consumer Complaint Response

3. ***Violations of Law and Consumer Harm***
   - Root Cause
   - Severity
   - Duration
   - Pervasiveness

The first two rating categories—Board and Management Oversight and Compliance Program—include factors related to the bank's compliance management system (CMS). Examiners will consider the size, complexity and risk profile of the bank when evaluating the effectiveness of the bank's CMS. Examiners will evaluate the four factors in the third category—Violations of Law and Consumer Harm—to determine the significance of the violations, including the level of consumer harm involved.

Will anything change during the examination process? For the most part, the compliance examination process will not change. Examiners will continue to evaluate the effectiveness of the bank's compliance management program, given the bank's compliance risks, and will assess the significance of any identified violations. The CC Rating System addresses several areas in more detail than before, such as how a bank anticipates and responds to changes that impact compliance, the process the bank has for receiving and responding to consumer complaints, how a bank manages third-party relationships and how a bank self-identifies and/or takes corrective action on violations or other compliance weaknesses noted.

Our SMBs will likely see a few additional changes during our examinations. For example, the format and content of the compliance examination report will change somewhat to help ensure that we sufficiently explain the bank's rating under the CC Rating System.

How banks can use the CC Rating System

The updated CC Rating System and the existing Community Bank Risk-Focused Consumer Compliance Supervision Program (Risk-Focused Program)[3] provide useful guidance for banks when evaluating the effectiveness of their own compliance management programs. Each assessment factor in the new CC Rating System definitions contains a description and list of actions that correspond to the five rating levels.[4] These descriptions provide details on factors that support particular ratings and help show how examiners will evaluate a bank's compliance management program. Banks may find it valuable to assess their own programs using these same factors. Similarly, banks can use the Risk-Focused Program as a guide for self-assessing compliance risks and determining the most effective controls to use for addressing these risks. Using the CC Rating System and the Risk-Focused Program as guides for compliance self-assessment reviews can help the bank identify potential issues and address them effectively through improvements to the bank's compliance program and/or operations.

Compliance resources

- CA 16-8: Uniform Interagency Consumer Compliance Rating System.
- CA 13-19: Community Bank Risk-Focused Consumer Compliance Supervision Program

---

[1] Federal Reserve System, Consumer Affairs (CA) letter 16-8.

[2] Under the rating system, a 1 rating represents the highest rating and consequently the lowest level of supervisory concern, while the 5 rating represents the lowest rating and consequently the most critically deficient level of performance and the highest degree of supervisory concern. Ratings of 1 or 2 indicate satisfactory or better performance. Ratings of 3, 4 or 5 indicate less-than-satisfactory performance. See CA letter 16-8.

[3] CA letter 13-19.

[4] FFIEC Guidance on the Uniform Interagency Consumer Compliance Rating System, CA letter 16-8.

SAFETY & SOUNDNESS UPDATE *continued from page 1*

securely transmit electronic files, we conduct a significant portion of bank examinations and holding company inspections off-site. The most recent phase in this evolution is banks' migration to electronic loan files. This change creates opportunities for us to conduct loan reviews off-site. When we do this, we are able to conduct the majority of the examination off-site, because we already complete most of the financial analysis off-site. Either way, we always have some on-site presence. (Please note that there is no requirement for banks to image loan files or for us to conduct the loan review off-site. Some bankers request that we review loans on-site so that their lenders have face-to-face time with examiners; we continue to accommodate these requests.)

Off-site work clearly has mutual benefits. It provides cost savings, lessens the travel burden on examiners and reduces the burden created by an on-site exam team. A related benefit that may not be apparent to banks is that it allows us to assign large training teams to exams without creating the space needs and disruption of a large training crew on-site. We then send smaller groups of trainees to the bank during the final on-site week to give them on-site exposure that is critical to their development as examiners.

The shift to off-site work is not without its challenges. One of the main challenges is conducting conversations by conference call. Poor connections, the inability to see nonverbal cues or difficulties referencing specifics in documents because neither party can easily "point" to a document can make the process difficult. The key to success for off-site examination work is good communication between bank management and examiners. To promote this, examiners work with our banks ahead of time to establish how contacts are made, by whom and how frequently communication will occur. To make conference calls more efficient and effective, examiners send questions in advance of meetings whenever possible, cover multiple topics in each meeting to reduce the number of meetings and, when something is too difficult to discuss over the phone, examiners pass it along to the team that wraps up the examination on-site.

Off-site work clearly has mutual benefits. It provides cost savings, lessens the travel burden on examiners and reduces the burden created by an on-site exam team. A related benefit that may not be apparent to banks is that it allows us to assign large training teams to exams without creating the space needs and disruption of a large training crew on-site.

Some banks have video conference capabilities that we would like to explore as an option on examinations. If you have the technology and are interested in using it for conference calls at your next examination, please let your relationship manager know before the examination to allow time to test the technology.

Feedback from bankers on our off-site work has been largely positive. Bankers appreciate the reduced burden on the bank. While the shift to more off-site processes changes where we complete the work, it does not change the tasks we complete. Completing more work off-site often requires banks to provide more information in advance of the examination to facilitate the off-site work; however, this offsets the information that bankers historically assembled and held on-site for examiner review. While bankers' feedback notes the more extensive advance requests, they also acknowledge the trade-off for less disruption at their bank.

Thank you for the feedback thus far and for working with us through these changes. Please continue to provide feedback or ideas on how we can continue to improve the examination experience.

NINTH DISTRICT HIGHLIGHTS *continued from page 1*

to conducting more examination work off-site. Some of the changes are due to advances in technology, but many of them also reflect the post-financial-crisis environment. Post-crisis, we began seeing fewer issues that required the immediate and direct attention of examiners. This is one example of how we have embraced change and how we adjusted course based on industry conditions, feedback and the environment. While we started implementing such changes over three years ago, our work on off-site examinations continues to evolve. This change has been easier for some to embrace than others, both for our own examiners and for our state member banks. Again, we have comfort in familiarity, and this change pushes us outside our comfort zone. Given the unknowns with the regulatory environment, we can and should expect ongoing evolution in the way we carry out our supervisory work.

Seeking input on change

In order to get more comfortable with and embrace change, particularly the unknowns, we must have strong avenues for two-way communication. We will continue to conduct Outreach events and will communicate with you through avenues such as this newsletter; however, we also need you to provide feedback and ideas to ensure that we have a strong understanding of the environments in which you operate. I encourage you to reach out to me directly, reach out to your relationship manager or submit comments and suggestions for improvements to our central email address: mpls.src.outreach@mpls.frb.org. If there's one thing we can count on, it is change. Please let us know how the changing environment and the unknowns affect you so that we can be in the best position to respond.

Common Cybersecurity Findings and How to Avoid Them

Rory Guenther, CISA - Senior Examiner
Patrick Doring and Greg Strom contributed to this article.

Strong cybersecurity controls continue to be extremely important due to the frequency of cyber attacks and the severity of losses that could result from a control breakdown. Headlines remind us almost daily of the ever-present and evolving cybersecurity risks facing financial institutions. State-sponsored hackers, botnets, distributed denial of service attacks, account takeovers, ransomware and good old-fashioned viruses are just a few of the threats you need to consider when evaluating your organization's risk and preparedness.

This article will discuss some of the common challenges illustrated in examination findings, highlight some measures you can take to proactively strengthen those areas in your organization and give a brief overview of how the Federal Reserve Bank of Minneapolis assesses cybersecurity risk.

Common examination findings

Cybersecurity risk assessments

We have observed many institutions in which management has not adequately assessed cybersecurity risk applicable to their organization nor appropriately communicated results and related action plans to the board of directors.

One effective tool bankers can use to conduct cybersecurity risk assessments is the Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity Assessment Tool (CAT).[1] The CAT is useful in identifying cybersecurity risk and determining the maturity level of a bank's cybersecurity preparedness. The baseline maturity level in the tool is characterized as meeting the minimum expectations required by law and regulations or recommended by supervisory guidance. We encourage you to utilize the CAT in completing this assessment, but it is not a supervisory requirement and you may use another method.

Virtualization/cloud technologies

Many banks are adopting virtualized and/or cloud technologies and often outsource work to third parties to install, configure and even manage these systems. The technologies allow banks to decrease costs and increase efficiency by reducing the need for physical servers and data center space. Virtualization allows multiple servers and applications to run on a single piece of physical hardware, while cloud computing uses virtualization to deliver shared computing resources—as a service and on-demand over the internet. We have noted a number of instances in which controls were not properly configured, documented or understood by the bank, and oversight of critical vendors was inadequate.

Examiners look for documentation and independent validation of security configurations and access levels for virtualization and cloud technologies. We also check for formalized vendor oversight programs, including defined data and hardware ownership, ongoing monitoring and reporting processes and data privacy expectations.[2]

Business resiliency

In today's environment, it is commonly held that the likelihood of preventing every type of cyber incident is close to zero. Sound resiliency planning, including incident response, business continuity and disaster recovery plans, is essential to mitigate the impact of a cyber incident on your organization. However, we continue to identify instances of outdated or inadequate business resiliency planning and testing.

Bankers can strengthen their organization's resiliency by ensuring plans are up to date and can be used for a wide range of events, including potential cyber events. Ensure that staff, management and vendors are aware of the plans and their responsibilities related to the plans. Test the plans periodically and include critical vendors, senior management, and both information technology (IT) and business line personnel.

Effective plans go beyond traditional disaster recovery testing, include tests throughout the year and incorporate a variety of scenarios such as tabletop exercises for potential cyber incidents. Your board of directors will want to hear the results and lessons learned, given the importance of this topic.

How do examiners assess your cybersecurity readiness?

The Federal Reserve System is now using the Information Technology Risk Examination (InTREx) Program for planning and conducting IT examinations at Reserve Bank–supervised financial institutions. InTREx is a collection of examination workpapers and modules used to assist in completing IT examinations. The FDIC is also using InTREx.[3]

InTREx is scalable, allowing examiners to use it for noncomplex as well as complex institutions. InTREx starts with a standardized IT risk profiling to determine the inherent risk rating and risk level. Based on the inherent risk level, examiners will include InTREx work programs and modules to appropriately assess risks in the IT examination scope.

InTREx requires an assessment of cybersecurity preparedness that ties to baseline controls identified in the CAT. In addition, InTrex guides examiners through an assessment of Section 501(b) of the Gramm-Leach-Bliley Act. Upon completion of the core modules, examiners will assign IT composite and component ratings based on the Uniform Rating System for Information Technology (URSIT).[4] The Report of Examination contains results from the assessment and any Matters Requiring Attention identified during the review.

---

[1] FFIEC Cybersecurity Assessment Tool, "Overview for Chief Executive Officers and Boards of Directors," June 2015, www.ffiec.gov/cyberassessmenttool.htm

[2] SR 13-19 / CA 13-21, "Guidance on Managing Outsourcing Risk," December 2013, https://www.federalreserve.gov/supervisionreg/srletters/sr1319.htm

[3] FDIC FIL -43-2016, "Information Technology Risk Examination (InTREx) Program, Enhanced Information Technology and Operations Risk Examination Procedures," June 2016, https://www.fdic.gov/news/news/financial/2016/fil16043.html

[4] SR 99-8, "Uniform Rating System for Information Technology," March 1999, https://www.federalreserve.gov/boarddocs/srletters/1999/SR9908.HTM