

Supervision News Flash

January 30, 2017

Creating IT Change Management Standards

In 2015 and 2016, we shared a series of articles on the top five IT examination findings. We concluded that original series last April by saying that we would get back to you periodically as new IT issues hit our radar.

We highlighted in our [December issue](#) that we've seen an increasing number of examination issues in the development and acquisition space. We covered project management expectations in that article, and now we're back with part two of this new series focused on the development and acquisition area: **change management**.

Technology systems are dynamic, and as such, controls should be in place to manage change. Change management encompasses change control, patch management, and system conversions, as well as your policies, procedures, and processes for implementing such change.

Matching standards with size and complexity

Like project management, an institution should develop change management standards to match its size and complexity. Regardless of size though, you should have written change management policies and procedures that are consistently applied.

Consistency contributes to a change management process that is **defined, managed, repeatable and optimized**. Risks associated with improper change management standards include serious degradation of IT performance, internal and external user dissatisfaction, accounting issues, reputation damage and critical operational disruptions.

Effective **change management standards** encompass:

- **Change Control:** Developing policies that address risk, testing, authorization and approval, timing of implementation, post-installation validation and back-out or recovery.
- **Patch Management:** Establishing procedures to stay current with patches, testing them in a segregated environment and installing them when appropriate.
- **Conversions:** Drawing on a number of control disciplines involving change processes and strategic planning, including project management, change control, testing, contingency planning, back-up, vendor management and post-implementation review.

In this arena, our examiners have found that the majority of our institutions haven't adopted change management standards. Developing and using a defined change management process will help you minimize the risks we've highlighted.

For specific questions on this topic or other IT related matters, please feel free to email Cara Mitchell, Operational Risk Managing Examiner, at Cara.Mitchell@rich.frb.org or call her at (804) 697-2627.

Resources include: [FFIEC IT Development & Acquisition and Operations Booklets](#).

You can also read all of our [previous articles](#) on IT examination issues on richmondfed.org

Planning for the Inevitable: Security Breaches

It seems like every time we've caught up on news recently, we're reminded that cyber-attacks are happening and they're affecting our financial institutions! The FFIEC has issued [two statements](#) focused on cyber-attacks, so please take time to read them to ensure you have appropriate risk management practices in place to effectively mitigate these attacks. Most importantly, it's critical that you have appropriate incident response procedures that align with regulatory guidance in the event of a cyber-attack on your institution.

What you should know

In 2005, the Federal Reserve issued a joint SR 05-23 and CA 05-10 Letter, [Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice](#), which outlines the requirements for an incident response program. The guidance also defines sensitive customer information and sets expectations for financial institutions in the event of a security breach involving unauthorized access to sensitive customer information.

Sensitive customer information is all that personal information that none of us wants made public. Access, as defined by the [FFIEC Information Security Booklet](#), refers to the ability to physically or logically enter or make use of an IT system or area — secured or unsecured — and is the process of interacting with a system.

We've recently learned that there's been some confusion about when to report an incident, because there was a misunderstanding about what 'access' really means. Access doesn't mean that customer information must have been transmitted; instead, it means that someone or something has entered your system(s) where customer information resides. **This is the key factor in whether or not to report the incident to your Federal regulator and potentially law enforcement.**

While our focus in this article is a cyber-incident, the incident-response guidance is broader than just reporting cyber incidents. It also covers things such as sending the wrong statement to a customer or accidentally emailing confidential information to a person outside of your organization.

What you should do

Be prepared, because you could be next! Review your incident response policies and procedures and ensure your employees are aware of — and well trained on — how to handle a security breach. Your organization's response plan should include:

- **Assessing** the incident to determine what system(s) and types of customer information may have been accessed or misused
- **Notifying** your primary Federal regulator ASAP when you become aware of an incident involving unauthorized access to or use of sensitive customer information
- **Complying** with BSA regulations to ensure appropriate suspicious activity reports are timely filed
- **Containing and Controlling** the incident
- **Determining whether you need to notify customers.** You may want to discuss this aspect with your legal counsel to determine if and when it's required to notify customers.

Questions?

If you have questions about your incident response procedures or you're trying to determine whether notification is required, contact Operational Risk Managing Examiner Cara Mitchell at cara.mitchell@rich.frb.org, or call her at (804) 697-2627 to discuss.

Considerations for Scenario Analysis at CRE Concentrated Banks

Over the past few years, we've observed that commercial real estate lending by Fifth District financial institutions is growing. At the same time, capital growth has not kept pace with the strong CRE loan growth at many of these banks.

As a result, concentration levels in CRE, particularly in construction and land development lending, have increased. This concentration growth has come against the backdrop of several robust and rapidly appreciating real estate markets within the Fifth District. On top of that, many institutions are increasingly allowing policy exceptions, or amending loan policy, to permit more liberal repayment terms.

These developments point to a heightened level of credit risk in CRE lending. While a real estate meltdown may not be imminent, it's generally prudent to consider the impact of adverse events, like a potential downturn, on your bank's financial condition, before such an adverse event occurs. That's where scenario analysis comes in.

Scenario analysis

As outlined in SR 07-1, "An institution with CRE concentrations should perform portfolio-level stress tests or sensitivity analysis to quantify the impact of changing economic conditions on asset quality, earnings, and capital." The scenario analysis should inform senior management and the board of directors about the current risk embedded within the CRE loan portfolio should certain adverse

conditions arise, and estimate the ability of the bank to withstand various stress events. These stress events may be expected — for instance based on past experience — or perhaps more importantly unexpected.

Scenario analysis usually takes the form of either a top-down or bottom-up approach. Combined with the appropriate assumptions and scenarios, either approach works. The top down approach usually involves selecting existing pools of homogeneous loans and stressing their loss rates. In the bottom-up approach, individual loan characteristics are stressed, and then portfolio losses are totaled from the individual loan loss calculations.

Regardless of the type of approach, there are **factors to consider** when developing and implementing an effective CRE scenario analysis process, such as:

- **Including all applicable loans** where repayment is based on income generated from, or sales of, the real estate collateral. This includes the construction and land development portfolio if a material concentration exists.
- Using a **range of potential scenarios**, including a severe adverse environment. These scenarios should consider possible outcomes, even if the institution has not experienced such an event in its recent history.
- Considering other income statement **impacts outside of direct credit write downs**. These might include reductions in interest income or additional noninterest expense.
- Including results from the **scenario analysis in capital and strategic planning**, as well as overall lending policy limits and guidelines.
- Incorporating the process into the **overall internal control environment**, including the audit/independent review or model validation process, as applicable.

The sophistication and scope of the analysis will vary depending on the size and risk profile of the portfolio. Nevertheless scenario analysis is a key component of the overall credit risk management framework for CRE concentrated banks and should be incorporated into overall corporate governance structure, including capital and strategic planning efforts. Effective and ongoing scenario analysis, as well as the other key elements in SR 07-1, during relatively prosperous times will provide a stronger position to withstand the next CRE downturn when it occurs.

Ask the Fed Session Feb. 1

The U.S. payments system is rapidly evolving and the changes affect banks of all sizes. The Federal Reserve System has worked with financial industry stakeholders since early 2015 on efforts to improve

the speed, security and efficiency of payments in alignment with the desired outcomes established in the *Strategies for Improving the U.S. Payment System* paper.

Because of the importance of this topic, we are bringing to you a special “Ask the Fed” session on **Wednesday, February 1, from 11 a.m. - Noon ET**. [Registration is now open at www.askthefed.org](http://www.askthefed.org).

Dan Gonzalez, vice president of the Payments Industry Relations Program, will discuss progress toward the desired outcomes, including accomplishments to date and upcoming milestones of the Faster and Secure Payments Task Forces.

As always, you can email your questions in advance of the session at questions@askthefed.org. We'll take questions during the session as well, but questions received in advance will receive priority.

New Supervision Contact System

We're in the process of ensuring that we have updated contact information for institutions supervised by the Richmond Fed so that we're able to share with you relevant supervisory guidance and other pertinent communications.

If you're the primary contact for your supervised institution, you'll soon be receiving a communication from us through the U.S. Postal Service asking you to confirm contact information for your organization. Please help us by sharing any changes as soon as possible.

On a related note, we have recently begun sending out SR Letter summaries and attachments to supervised institutions via email. Rest assured that these emails are from us, and we believe you will benefit from these communications. If you have any questions regarding the content of any SR or CA letters please reach out to your relationship team contact or Central Point of Contact.

Recap of Recent Supervision and Regulation Guidance

Supervision and Regulation Letters, commonly known as SR Letters, address significant policy and procedural matters related to the Federal Reserve System's supervisory responsibilities. Consumer Affairs letters address significant policy and procedural matters related to the Federal Reserve System's consumer compliance supervisory responsibilities. Active [SR](#) and [CA](#) letters are listed in reverse chronological order. Here are recently issued guidance letters:

[SR 17-2](#)

Updates to the Expanded Examination Cycle for Certain State Member Banks and U.S. Branches and Agencies of Foreign Banking Organizations

[SR 16-19](#)

Frequently Asked Questions on the Current Expected Credit Losses Methodology (CECL)

[Richmond Fed President Jeffrey Lacker Announces Retirement](#)

Jeffrey M. Lacker, president and chief executive officer of the Federal Reserve Bank of Richmond, announced that he will retire on October 1, 2017, after 28 years of public service at the Richmond Bank. Dr. Lacker joined the Richmond Fed in 1989 and served in various leadership positions prior to this appointment in August 2004

Richmond Fed's Board of Directors formed a search committee that will be led by Margaret Lewis, Board chair. The search firm of Heidrick & Struggles has been engaged to assist the committee in conducting a nationwide search to identify a broad, diverse and highly qualified candidate pool for this leadership role. Individuals from both inside and outside the Federal Reserve System can apply. The public can make submissions directly to the search firm through the Bank's public website, richmondfed.org/presidentialsearch.

For more information on Supervision News Flash [subscribe](#), or contact [Hamilton Holloway](#). The Supervision News Flash is an occasional publication of the Richmond Fed that provides information on topics and trends affecting financial institutions as well as Supervision, Regulation and Credit throughout the Fifth Federal Reserve District.