

Supervision News Flash

December 2, 2016

IT Hot Topics Continued...

Over the past 18 months, we updated you on our top five IT findings. Since then we've seen issues appearing in the development and acquisition area related to project and change management. As always, our goal is to help you better prepare for your next examination, so we'll cover these new issues in two updates, and we'll first cover project management.

To set the stage, the [FFIEC Development and Acquisition Booklet](#) notes that, "Development and acquisition is defined as an organization's ability to identify, acquire, install, and maintain appropriate IT systems." The process includes the internal development of software applications or systems and the purchase of hardware, software or services from third parties.

Project management standards

Technology is constantly evolving and plays a significant role in the success of our financial institutions. While project management standards don't guarantee that organizations will appropriately develop, acquire, and maintain technology systems, standards enhance your control over projects, thereby decreasing project risks.

Well-defined project management standards help ensure systems are obtained in an efficient manner, operate in a secure environment and meet organizational and end-user needs. It's a best-practice to develop project management standards based on the size and complexity of your institution and based on the project's features and risks. Without proper standards, associated risks include ineffectively managed projects, cost overruns, inferior technology systems, and the possibility of loss resulting from inadequate processes, personnel or systems.

Developing well-defined plans for all projects with effective **project management standards** include:

- **Project Planning:** describing existing system benefits and weaknesses, explaining project goals, and identifying user, information, system, and network requirements. Keep in mind that project plans should detail cost, staffing, resource and training requirements, and should be well-defined for all projects.
- **Configuration Management:** requiring the identification of baseline configurations (original versions) of hardware, software, services, documentation and project management plans.

- **Quality Assurance:** addressing *commitment* from all involved parties; *completeness* — each phase of a project includes procedures to follow and items to deliver; *scalability* — QA standards should match project characteristics and risks; *measurability* — assess results against defined expectations; *tracking* — properly record, report and monitor problems; and *independence* — audit and QA should be independent of the project they review.
- **Risk Management:** including procedures for identifying and managing internal and external project risks.
- **Testing:** establishing testing standards that require the use of predefined, comprehensive test plans, end-user involvement and documented test results.
- **Documentation:** maintaining documentation for all technology resources, including nontechnical policy and procedural guidance, and technical information such as hardware and software configurations, and system and application source codes.

In this area, our examiners have found that many institutions haven't established project management standards and have no formal documentation to support projects that are in process or have been completed since the previous examination.

Formal, detailed project management standards not only enhance the success of a financial institution's information technology initiatives, but also provide for the establishment of key controls and standards that help mitigate operational risk.

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 Booklet](#).

Fed Updates Risk Management Guidance for Banks

With the issuance of [SR letter 16-11](#) in June, the Federal Reserve System updated its guidance on risk management for all Fed-regulated institutions with total assets of less than \$50 billion. This new guidance replaces our prior guidance on risk management, [SR letter 95-51](#).

We want to highlight changes in the guidance that will have an impact on how we'll assess risk management at your organization going forward for examinations and inspections.

First, as you probably recall, we have six primary risk indicators we use in our overall risk evaluation, but one of them has changed. **Reputational risk has been replaced with compliance risk.** The other unchanged primary risks are **credit, market, liquidity, operational and legal risk.**

This new guidance defines compliance risk as *"the risk of regulatory sanctions, fines, penalties or losses resulting from failure to comply with laws, rules, regulations, or other supervisory requirements applicable to a financial institution."*

Compliance risk broader than consumer

Compliance risk is broader than just consumer compliance, so while examiners are able to factor in consumer compliance to the overall assessment of compliance risk, this is not intended to signal that

our examinations are going to be conducted concurrently, or that our findings are intended to revolve solely around consumer compliance.

Reputational risk, while no longer a primary risk factor, can still occur when a risk management gap in a primary risk exposes the institution to adverse publicity. In these cases reputational risk would be addressed within the discussion of the primary risk.

Key elements of sound risk management

The key elements of a sound risk management program have not changed. Examiners will continue to assess board and senior management oversight; policies, procedures and limits; risk monitoring and management information systems; and internal controls. Likewise, the rating scale for risk management has also not changed.

The other change you'll notice in the new guidance is that the language defining these key elements has been updated and clarified. Supervisory expectations on the risk management roles and responsibilities of the board of directors and senior management have also been clarified and more clearly delineated.

So be on the lookout in your upcoming reports of examination for the assessment of compliance risk instead of reputational risk, and clearer delineation of issues on the roles and responsibilities of senior management versus the board of directors in addressing the examination issues. You can find this guidance [here](#). If you have questions regarding the new guidance or its application, please reach out to your Richmond Fed portfolio team or central point of contact.

Now Search FR Y-6 Reports Online

We've just added [FR Y-6 \(Annual Report of Holding Companies\)](#) report submissions to [RichmondFed.org](#). This new feature allows you to browse by year, and search by RSSD or holding company name with immediate access rather than requesting information by email.

As you know, the Federal Reserve uses a wide range of tools to collect data from bank holding companies, depository institutions, other financial and non-financial entities and consumers. Collected data is used for monetary policy development, supervision and regulation of the banking industry and protection of consumers' rights.

Ask the Fed Session Dec. 20

It's that time again for our year-end economic update with Dr. Dave Altig, director of research and executive vice president of the Federal Reserve Bank of Atlanta.

The state of the U.S. economy affects every financial institution in the country, regardless of your location. Your lending decisions, as well as your business plans, are all impacted by the economy. Dave returns to "Ask the Fed" to provide an update on current economic conditions, provide his forecast for 2017, and take your questions too.

The session will be **Tuesday, December 20, from 3-4 p.m. ET**. [Registration is now open at www.askthefed.org](http://www.askthefed.org).

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

Inaugural Community Banking Technology Forum Highlights

The Federal Reserve Bank of Richmond hosted its inaugural Community Banking Technology Forum to bring together community-bank IT professionals to discuss issues and concerns that bankers deal with on a regular basis.

The September event kicked off with opening remarks by Mark Mullinix, first vice president and chief operating officer of the Richmond Fed. The morning sessions included a presentation on the risk and rewards associated with cloud services, followed by a regulatory town hall where discussions encompassed examination hot topics and provided the 130 attendees an opportunity to ask questions of the regulators. The afternoon sessions covered:

- Leadership approaches in disaster recovery
- A roundtable on cybersecurity and its impact on the information security program
- [Financial Services Information Sharing and Analysis Center's](#) (FS-ISAC) cyber information sharing program
- Payment systems risk
- Recent cybersecurity threats and concerns.

The key takeaways shared by the majority of the speakers were the importance of maintaining up-to-date systems, effective patch management programs, and appropriate controls over system access. To review speaker bios and presentations, visit us at <http://www.CBTF.com>.

One of the most memorable comments from an attendee was, "To hear and see how much work we at our bank have left to do and how we will be viewed by regulators if we don't improve our efforts, but mainly how much unnecessary risk we are taking by not following the guidance given."

Based on the overwhelmingly positive responses, we're evaluating plans for our next forum. If you have questions about or suggestions for the forum, please contact us at CBTech@rich.frb.org or reach out to Operational Risk Managing Examiner Cara Mitchell at cara.mitchell@rich.frb.org or call her at (804) 697-2627.

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 16-16 / CA 16-7](#)

Special Post-Employment Restriction for Senior Examiners

[SR 16-15](#)

Exception to Appraisal Regulation Requirements in Areas Affected by Flooding in Louisiana

[CA 16-8](#)

Uniform Interagency Consumer Compliance Rating System

Last [Beige Book](#) of the Year

Informal review by the Federal Reserve Banks of current economic conditions in their Districts
<https://www.federalreserve.gov/monetarypolicy/beigebook/default.htm>

Commonly known as the Beige Book, this report is published eight times per year. Each Federal Reserve Bank gathers anecdotal information on current economic conditions in its District through reports from Bank and Branch directors and interviews with key business contacts, economists, market experts and other sources. The Beige Book summarizes this information by District and sector. An overall summary of the twelve district reports is prepared by a designated Federal Reserve Bank on a rotating basis.

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.