

## Supervision News Flash

September 2, 2015

### IT Hot Topics for Exams – second in a series

If you couldn't tell that Information Technology is a big issue based on the [January 2015 Supervision News Flash](#) then maybe this installment will do the trick. (That News Flash covered risk assessments and board reporting as well as patch management.)

As a refresher we're covering the most common examination issues in a series so that you can be better prepared for your next examination. This time we'll discuss topics that rank #2 and #3 on the list of most common examination findings: Important factors you need to know about **vendor management** as well as **network and core access, administration and security**.

Cybersecurity continues to be the buzzword in the IT world with new threats and attacks in the news daily. The rapidly changing technological environment and the dependence on technology to provide customers with a variety of products and services, some of which are outsourced, has resulted in an increased reliance on external service providers. This reliance means it's even more critical to have an effective vendor management program. As a result, it's very important for bank leaders to review their risk management practices and controls over vendor management, as well as over IT networks and authentication, authorization and fraud detection to protect your information assets.

As you read on and find yourself wanting more information on either of these issues, or on other IT related matters, please feel free to email [Cara Mitchell](#), Operational Risk Managing Examiner, or call her at (804) 697-2627.

### Vendor Management:

While outsourcing has many benefits for banks and their customers, outsourcing is not without risks such as information security breaches, loss of funds, damaged reputations or even loss of competitive advantage. Your decision to outsource should mesh with your organization's strategic plan and corporate objectives.

And while outsourcing and the use of external service providers may make sense for your bank, your board and senior management are still accountable for oversight of the various vendors and the vendor management program to ensure the outsourced activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations.

The **most common** issues examiners have identified in this area include:

- **Board and senior management oversight:** As members of the board and senior management, you should ensure that you have adequate risk mitigation practices in place for oversight and management of outsourcing relationships, including establishing effective VM policies and

procedures, and ensuring compliance with applicable laws and regulations. Boards should approve their programs at least annually, while senior management should ensure the policies are executed and that they follow through on regular board reporting. *In this area our examiners periodically find that a formal VM policy customized for your bank's current practices hasn't been developed; that there's non-existent board reporting or that board reporting is ineffective because it doesn't cover material matters related to the program.*

- **Risk assessments:** Risk assessments should assess the benefits and risks of outsourcing the proposed activity, evaluate how the outsourced relationship will be managed, and determine cost implications for establishing the outsourcing relationship. The risk assessments should be comprehensive and updated at appropriate intervals consistent with the VM program. *In this area our examiners most commonly find that the list of vendors needing an assessment is incomplete; the vendor risk assessments aren't comprehensive; or it's not clear what methodology you're using to prepare the assessment.*
- **Oversight and ongoing monitoring:** You should establish an effective oversight program to monitor each service provider relationship, and set acceptable performance metrics. This monitoring should be well-documented by people with appropriate expertise. Base your risk-focused monitoring level and frequency on the complexity of the provided service. *In this area our examiners most commonly find vendor monitoring that isn't risk-focused, documented or supported; and inadequate ongoing vendor monitoring requirements.*

In 2013 the Federal Reserve issued SR Letter 13-19, [Guidance on Managing Outsourcing Risk](#). This guidance expands the scope of the VM program to include all outsourced service provider relationships, regardless of the type of bank activity. Additionally, the guidance outlines the most important elements of an effective VM program. Your VM program should be risk-focused, concentrating on those outsourced activities that have a substantial impact on your bank's financial condition; are critical to your bank's ongoing operations; involve sensitive customer information or new products or services; or pose material compliance risk.

While not making our list of most common issues we're seeing, these core elements of the VM program are nonetheless important, so here's what you also should be considering as you evaluate your own program — **due diligence and service provider selection, contract provisions and implementation, incentive compensation reviews, and business continuity and contingency plans**. See [SR 13-19](#) for more details on these topics.

Resources include: [FFIEC Outsourcing Technology Services Booklet](#); SR 00-17, [Risk Management of Outsourced Technology Services](#); and, SR 13-19, [Guidance on Managing Outsourcing Risk](#).

## Network and Core Access, Administration and Security:

Information is arguably one of your financial institution's *most important* assets, so you should properly safeguard it. It's necessary to protect those assets to establish trust between your institution and your customers, maintain compliance with laws and regulations, and protect your reputation. Security is an ongoing process, and the condition of your controls is just one indicator of your overall security posture. You protect your information by instituting a security process that:

- *identifies* risks,
- forms a strategy to *manage* the risks,
- *implements* the strategy,
- *tests* the implementation and
- *monitors* the environment to *control* the risks.

The goal of access control is to restrict access to only authorized individuals and devices, and then limit their activities to the minimum required for business purposes. Failure to restrict access beyond the minimum required for work to be performed exposes your institution's systems and information to a loss of confidentiality, integrity and availability. That, in turn, exposes you to increased operational, reputational and legal risk from threats including customer information theft, data alteration, system misuse and denial of service attacks.

So it's necessary to periodically update and review access rights since they don't automatically expire or update. You should update when an individual's business needs for system use change. These periodic and documented user-account reviews are a required control to test whether access rights are aligned with job responsibilities.

The most common issues examiners have identified with the **network** — the communications infrastructure that houses the core and facilitates core system processing — include the following:

- Administrative privileges are granted to employees at the workstation level
- Multiple users share an administrator account
- Network administrator activity isn't adequately monitored
- Network access reviews aren't completed, documented or performed by an independent party

From a **network** access, administration and security standpoint, examiners have set the following expectations you should be considering as you evaluate your own systems — though it's not all-inclusive:

- Regularly update network diagrams and include all access points
- Implement effective firewalls, intrusion detection and intrusion prevention systems
- Have appropriate controls on remote access devices and network access points
- Ensure effective password complexity
- Establish periodic, documented independent reviews of user access, server event logs, network event logs and network administrative activity
- Provide appropriate oversight of administrators, users, file changes and security settings

The most common issues examiners have identified with the **core** — core banking software/system or core transaction processing system — include the following:

- Core system access rights are excessive and not assigned based on job responsibilities
- Core system reviews do not encompass all core accounts and are not completed annually
- Core system reviews — including core system maintenance reviews — are not completed, documented or performed by an independent party

From a **core** access, administration, and security standpoint, examiners have established the following expectations — though it's not all-inclusive:

- Limit the number of employees with access to operating systems and set access rights that align with business needs
- Implement an effective process for assigning, changing and removing user access
- Use operating system security and logging capabilities
- Have an independent party perform logging and monitoring access and security events
- Update operating systems with security patches and appropriate change control mechanisms

Resources include: [FFIEC Information Security Booklet](#) and [FFIEC Operations Booklet](#)

**Stay Tuned...** The next News Flash will cover the topic that ranks #1 on the list of most common IT findings: **Disaster Recovery/ Business Continuity Planning**.

---

## Clarifying Expectations for Internal Audit

Recently here at the Richmond Fed we've received a number of queries from bankers, internal auditors and external accounting firms concerning [SR Letter 03-5 Amended Interagency Guidance on the Internal Audit Function and Its Outsourcing](#) as well as sections 1010.1 and A1010.1 of the [Commercial Bank Exam Manual](#). Figuring that many readers may have similar questions, and to help ensure a consistent interpretation and application of the policy statements, here's highlights that address the most frequently asked questions.

## Professional Standards

SR 03-5 (on page 3) introduces this topic by saying that, "Directors should consider whether their institution's internal audit activities are conducted in accordance with professional standards, such as the Institute of Internal Auditors' *Standards for the Professional Practice of Internal Auditing*." The guidance references the specific areas of the IIA standards, then goes on to say that bankers, "...should ensure that the following matters are reflected in their institution's internal audit function," – structure; management, staffing and audit quality; scope; communication; and contingency planning. SR 03-5 provides additional guidance on each of these topics.

## Oversight of Outsourced/Co-Sourced Arrangements

Bottom line: An institution can outsource the internal audit work but not the responsibility. Within the "Structure" section of SR 03-5, it covers that, "The audit committee should assign responsibility for the internal audit function to a member of management who understands the function and has no responsibility for operating the system of internal control." Page 7 of the guidance introduces the topic of outsourcing/co-sourcing arrangements and states that management, "...is responsible for approving the audit scope, plan and procedures ..." and "... is responsible for the results of the outsourced audit work, including findings, conclusions and recommendations." So that means a member of management is responsible for overseeing the outsourced arrangement. Additional guidance on this topic can be found in [SR 13-19 Guidance on Managing Outsourcing Risk](#).

## Audit Opinion/Conclusion

The internal auditor's responsibility to evaluate control systems and ongoing operations carries with it an obligation to report the results of that evaluation. The Management, Staffing and Audit Quality section of SR 03-5 (found on page 5), indicates that the manager of internal audit is responsible for an audit report that presents, among other things, "the results of the audit, including findings, conclusions and recommendations." This aligns with the "Oversight" expectations. Additionally, the *CBEM Section A.1010.1* outlines communication standards (on page 2) and says, "Each audit report shall contain an

opinion on the adequacy, effectiveness and efficiency of the systems of control and the quality of ongoing operations ... or an explanation of why an opinion cannot be expressed.” Requiring auditors to express an opinion or conclusion enables the board of directors and management to assess the reliability of the control systems and ongoing operations.

## **Applying the Internal Audit Expectations**

Both *SR 03-5* and *CBEM Section A.1010.1* are applicable to banks of any asset size since an effective system of internal control alongside an independent internal audit function form the foundation for safe and sound operations. You should have an internal audit function that is appropriate for your size and the nature and scope of your activities.

If you have questions or need additional information, please contact [James Clark](#) with the Richmond Fed.

---

## **Quick Reminder on Importance of Board Minutes**

Rest assured our goal is not to require board minutes to resemble the tax code in terms of detail and length. The goal is to ensure that they accurately reflect the record of your institution and the robustness of your discussions.

Basically minutes should record your board’s actions over time, remind current directors of previous actions and provide continuity for future directors. So we’re sharing some highlights on the importance of adequate record keeping for both board and board committee meetings.

The process by which your board of directors undertakes decision making and the manner in which those decisions are documented are as important as the decision itself. Examiners sometimes note that, based on their review of board and board committee minutes during examinations and inspections, the minutes are fairly cursory.

In certain instances the minutes have not reflected the substantive discussions or analysis that reportedly occurred on important topics such as strategic initiatives, senior level personnel decisions, problem credits, material funding issues or litigation matters. While it is important to document the board’s actions, minutes are not expected to be transcripts either.

Board minutes, as well as the minutes of board committees, constitute the official record of your institution and are a critical element of corporate governance that, among other factors, demonstrates the level of director involvement and helps substantiate that your board is fulfilling its fiduciary responsibilities. That means minutes should be sufficiently detailed to reflect the substantive discussions amongst board members and the decisions reached on important matters.

This should include financial and trend analysis information on critical components such as capital, asset quality metrics, earnings performance, liquidity position and sensitivity to market risk, since trend analysis is an important focus on examinations and inspections. The minutes should also reflect your directors' interest and involvement in the board committees — particularly audit committee minutes — to ensure management takes appropriate action.

The importance of maintaining adequate record keeping and strong minutes is referenced in both the [Commercial Bank Examination Manual](#) and the [Bank Holding Company Supervision Manual](#). Section 5000.1 of the CBEM covers how the board of directors should ensure that an accurate, adequate record of its actions is maintained. Both manuals indicate that part of the examination and inspection process should include a review of the minutes of the board and committee meetings, as well as the information packages for these meetings, to ensure board members are receiving adequate information and making informed decisions.

Additionally, [SR 95-51](#) (check out page 5) outlines the elements of sound risk management, one of which is active board oversight. One measure of active board oversight is maintaining adequate record keeping (found on page 7). Note that meetings conducted by telephone, if allowable by state law, should be documented as thoroughly as regular meetings.

---

## **Discount Window Seasonal Lending**

The Richmond Fed offers a seasonal lending program to assist healthy institutions in meeting cyclical funding needs caused by seasonal loan demand as well as seasonal deposit declines. Institutions experiencing regular and recurring seasonal liquidity pressures while serving customers engaged in cyclical businesses, such as agriculture or tourism, may find this program beneficial.

We use a variable, market-related interest rate for the program that is based on the average of the federal funds rate and the secondary market rate for 90-day CDs. Based on those market changes, we adjust the rate at the beginning of each two-week reserve maintenance period. For reference, the seasonal credit rate currently is at 0.20 percent. To receive seasonal advances under the program, you need to have current borrowing documentation on file and pledge sufficient collateral. Here's some general guidelines:

- The need arises from an expected movement in loans and deposits
- The need lasts for at least four weeks and generally does not exceed nine months
- The need exceeds a deductible percentage of deposits (call us for details)
- The program won't normally be available to institutions with deposits of \$500 million or more

If you're interested in learning more or beginning the qualification process, email [Michelle Turner](#) or call her at 800-526-2036.

---

## **Mark your calendars for the 2015 Community Bankers Forum**

The Richmond Fed will host a two-day Districtwide Community Bankers Forum on **November 12<sup>th</sup> and 13<sup>th</sup>**. The event, held in Richmond, will cover a number of hot banking topics and will include two

keynote sessions. You'll learn more details as we get closer to the event, but be sure to mark your calendar now.

---

## **Recap of Supervision and Regulation Guidance Issued this Year**

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. The letters are sent to banking supervision staff at the Board and the Reserve Banks and, in some instances, to supervised banking organizations. Active SR and CA letters are listed [here](#) in reverse chronological order.

Here are recent guidance letters issued this year:

[SR 15-9](#): FFIEC Cybersecurity Assessment Tool for Chief Executive Officers and Boards of Directors

[SR 15-8](#): Name Check Process for Domestic and International Applications

[CA 15-4](#): Expiration of the Protecting Tenants at Foreclosure Act

[CA 15-3](#): Revised Interagency Examination Procedures for Regulation Z and Regulation X

---

**For more information on Supervision News Flash** or to subscribe, please contact [Hamilton Holloway](#).

The Supervision News Flash is an occasional publication of the Federal Reserve Bank of Richmond that provides information on topics and trends affecting financial institutions as well as Supervision, Regulation and Credit throughout the Fifth Federal Reserve District.