



Supervision News Flash

January 28, 2015

IT Hot Topics for Exams – *first in a series*

The word is out on the street that operational risk, specifically Information Technology, is the **hot** topic on Safety and Soundness exams. While operational risk has always been one of the six key risks that examiners evaluate, it has been in the spotlight over the past year as a result of major headlines in the daily news about cybersecurity, information security breaches and disaster recovery planning. As the financial industry continues to expand its reliance on technology to meet business needs, and the technological environment continues to evolve rapidly and become more complex, IT will continue to be a focal point for examiners. In an effort to better prepare community bankers for examinations, and hopefully keep your banks out of the headlines, **we're going to cover the five most common IT findings**, as well as examiners' expectations, over the next several News Flashes. Each News Flash will cover one or two of the most common issues. For more information on any of these issues, please feel free to reach out to Cara Mitchell, Operational Risk Managing Examiner, at 804-697-2627, or Cara.Mitchell@rich.frb.org.

Today's News Flash topics rank #5 and #4 on the list of the most common examination findings from 2013-2014, with info you need to know about Information Security **Risk Assessments and Board Reporting**, as well as **Patch Management**.

Information Security Risk Assessments and Board Reporting:

The most common issues examiners have identified in this area are that the risk assessments frequently do not adequately identify and assess all customer information assets, and required information security board reporting is not comprehensive or completed annually.

Information is arguably a financial institution's *most important* asset and as such should be properly safeguarded. One of the keys to protecting information is the information security risk assessment, which is used to identify and understand risks to the confidentiality, integrity and availability of information and information systems. This risk assessment should also serve as a forward looking tool for management to help guide strategies to develop, implement, test and maintain the institution's information systems security position. While the initial development and implementation of the risk assessment usually requires the most significant time and effort, the risk assessment process should be an ongoing and dynamic part of your information security

program. As a critical component, your board should approve written information security policies, and the written report to your board describing the overall status and effectiveness of the information security program must be presented **at least annually**.

The risk assessment process is a relatively simple, three-step-process that will be evaluated by examiners as follows:

- **Gather the necessary information:** The risk assessment should be based on **current** and **detailed** knowledge of your institution's operating and business environments and should identify the information and the information systems to be protected, including electronic systems and physical components used to access, store, transmit, protect and eventually dispose of information. Information and information systems can be both paper-based and electronic.
- **Analyze the information:** The risk assessment should assess the relative importance of your various information systems based on the nature of their function, the criticality of data they support, and the sensitivity of data they store, transmit or protect. It should assess potential threats and vulnerabilities to your information systems, and identify controls that will mitigate the impact or likelihood of each identified threat exploiting a specific vulnerability.
- **Assign Risk Ratings:** The risk assessment should assign risk ratings to your information and information systems based on the probability or likelihood of an event occurring and the impact the event would have on your financial institution. You and your management team should consider internal controls when assigning ratings. The risk assessment should prioritize the risks present to determine the appropriate level of training, controls and assurance necessary for effective risk mitigation.

The annual report to your board that describes the status of the Information Security Program should address the information security risk assessment in addition to five other factors:

- Risk assessment
- Risk management and control decisions
- Service provider arrangements
- Results of testing
- Security breaches or violations and management's responses
- Recommendations for changes in the Information Security Program

Resources: *FFIEC Information Security Booklet, SR 01-15, Interagency Guidelines on Establishing Standards for Safeguarding Customer Information; SR 05-23, Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*; and, *Regulation H of the Board of Governors of the Federal Reserve Systems (12 CFR 208, Appendix D-2)*

Patch Management:

Maintaining accurate, up-to-date hardware and software inventories is a critical part of all change management processes. **Patching is critical!** The most common issues examiners find in this area focus on tracking and monitoring patches. Findings have ranged from non-existent or ineffective patching to patches not being applied in a timely manner. In addition, non-Microsoft systems may be overlooked and not patched, or board reporting related to patching is not completed or comprehensive.

The *FFIEC Development and Acquisition Booklet* provides specific guidance on an effective patch management framework, and is outlined below. These are the standards that examiners use to evaluate the effectiveness of your patch management program:

- **Identification**- identify and acquire patches from trusted sources
- **Evaluation**- evaluate the impact of installation of patches
- **Authorization**- approve patches; if a patch is not approved, document the support for reason(s) why the patch was not approved
- **Testing**- test all patches to minimize disruptions
- **Installation**- maintain appropriate back-up and back-out procedures
- **Documentation**- document software changes and maintain post-implementation evaluations and documentation

Stay Tuned... The next News Flash will cover topics that rank #3 and #2 on the list of most common IT findings: **Vendor Management** and **Core and Network Access and Administration**.

For more information on any of these issues, please feel free to reach out to Cara Mitchell, Operational Risk Managing Examiner, at 804-697-2627, or Cara.Mitchell@rich.frb.org.

SECURITY BREACH/ BANKERS BEWARE

In December a State Member Bank in the Fifth District was subjected to an ATM skimming incident that affected multiple ATMs. The institution notified the Richmond Fed per their incident response program and the event also was highlighted in regional news. In response to the incident, the bank restricted ATM activity for about 3,000 customers. Also an undisclosed number of accountholders experienced unauthorized activity on their accounts. Unfortunately this is not the first bank in our District to be affected by this rapidly-increasing type of activity, so we want to warn our community banks to be on the look-out.

The financial impact from ATM skimming can be substantial as highlighted in a New York case several years ago that resulted in the perpetrators stealing about \$1.8 million from customer accounts. Some current estimates peg ATM skimming losses in the U.S. at almost \$1 billion annually.

What you should know

Criminals target a bank and often send people to multiple ATMs to install skimming devices and cameras – usually on a Thursday or Friday. They then collect information such as card numbers and PINs, and remove the hardware before the start of business on Monday. The captured card numbers and PINs are then usually used in larger cities such as New York, Baltimore and Washington, DC to remove cash at ATMs or pay for purchases, which ultimately result in losses borne by your financial institutions.

What you should do

Both the bank involved in this most recent incident and the Richmond Fed want you to know about these incidents so you can alert your employees and customers. Pay special attention to your ATMs and look for unusual devices that may be attached to the card reader, the keypad, or any other part of the ATM – you might be surprised at what a 3-D printer can produce. You may want to increase the number of ATM inspections per day and tighten daily transaction limits for ATM usage outside of your bank’s market area. Such actions may help minimize losses to your financial institutions.

Questions?

Contact Operational Risk Managing Examiner Cara Mitchell at cara.mitchell@rich.frb.org, or 804-697-2627.

Regulation O Reminder – Loans to Executive Officers

Examiners will be looking more closely at the terms of these executive officer borrowings on examinations to ensure lending practices include the call features for loans made to these individuals. Bank management is urged to review executive officer loans to ensure lending practices align with the regulation. Please feel free to reach out to your Richmond Fed contact with any questions you may have regarding Reg. O.

[Section 215.5\(d\)\(4\)](#) of this regulation explains that all loans to executive officers should be ... “made subject to the condition in writing that the extension of credit will, at the option of the member bank, become due and payable at any time that the officer is indebted to any other bank or banks in an aggregate amount greater than the amount specified for a category of credit” that’s listed in the reg.

Multi-Family Loan Reporting on Schedule RC-R

In several Richmond Fed examinations last year, we noted that banks are including certain loans in the 50 percent risk weighting bucket, for risk-based capital calculation purposes, without ensuring these loans meet all of the required criteria for inclusion.

For loans that do not qualify, examiners will ask you to report these loans in the 100 percent risk weighting category. If the level of loans that are reassigned is significant, this could also lead to

a request to refile the Call Report. Additionally, the reassignment to a higher risk category may have a significant negative impact on a bank's risk-based capital ratios. For institutions with lower capital ratios, this decline in capital ratios may be material enough to affect the capital rating.

Examiners have primarily noted this issue in multi-family loans. These loans may be included in the 50 percent risk weighting bucket, though they must meet some fairly rigorous criteria. Since our examinations are looking at this issue more routinely now, **your management team is encouraged to consult not only the [Call Report instructions](#) but also the [Capital Adequacy Guidelines](#)** where you'll find additional criteria for including loans in the 50 percent risk bucket. Also reach out to your Richmond Fed contact with any questions you may have.

Federal Regulatory Agencies Announce Additional EGRPRA Outreach Meetings

Federal regulatory agencies have once again started the *Economic Growth and Regulatory Paperwork Reduction Act of 1996* review process, designed to identify outdated or otherwise unnecessary regulations. The agencies held their first outreach meeting last December in Los Angeles. **The next meeting is February 4, in Dallas.** Additional meetings are currently scheduled for Boston on May 4, Chicago on October 19, and **Washington, D.C. on December 2.** The agencies also plan to hold an outreach meeting in Kansas City this summer focused on rural banks. These meetings may be viewed live online at <http://egrpra.ffiec.gov/>.

Each meeting will feature panel presentations by industry participants and consumer and community groups. It also provides an opportunity for interested persons to present their views on any of the 12 categories of regulations listed in a June 2014 Federal Register notice that started the EGRPRA public comment process. Comptroller of the Currency Thomas Curry, Federal Reserve Governor Jerome Powell, and FDIC Chairman Martin Gruenberg are scheduled to attend the meeting in Dallas. In addition, Commissioner of the Texas Banking Department Charles Cooper will attend, and state banking regulators are invited to participate through the State Liaison Committee of the Federal Financial Institutions Examination Council (FFIEC). Additional information about the EGRPRA review process is available on the EGRPRA website: <http://egrpra.ffiec.gov/>.

Recent Guidance Letters Issued by the Board of Governors of the Federal Reserve System

[SR 14-10](#): Release of the 2014 Federal Financial Institutions Examination Council's Bank Secrecy Act/Anti-Money Laundering Examination Manual

[SR 14-9](#): Incorporation of Federal Reserve Policies into the Savings and Loan Holding Company Supervision Program