FEDERAL RESERVE BANK OF RICHMOND

Richmond • Baltimore • Charlotte

Supervision News Flash

April 29, 2016

IT Hot Topics for Exams- *third in a series*

We started this series as a way to highlight the most common IT examination issues from 2014 and 2015, and billed it as a three part series. So this article closes out that original series by addressing the number one issue from our original list: disaster recovery/business continuity planning.

Since we began this series though, additional IT issues have arisen that we believe deserve some air time as well. Watch for our News Flash in the coming months for information on those other IT issues. As always our goal is to help better prepare you for your next examination. So without further ado here's the number one topic on our list: Important factors you need to know about **disaster recovery/business continuity planning**.

Disaster Recovery/Business Continuity Planning:

The **business continuity planning process** should focus on the recovery of each critical business function and the supporting technology. You should develop a business continuity plan based on the size and complexity of your institution that's consistent with your overall business strategy.

The goal of the BCP should be to minimize financial losses, serve customers and financial markets with minimal disruptions, and mitigate the negative effects of business operations disruptions. As members of the board and senior management, you have ultimate responsibility for the business continuity planning process outlined below, as well as ensuring employees are trained and aware of their roles in its implementation. *In this area, our examiners periodically find that employee training hasn't been conducted.*

The planning process includes:

- **Business Impact Analysis —** You should regularly update your business impact analyses to reflect your institution's current operating environment. Leaders should ensure that the BIA:
    - Assesses all business functions and processes
    - Identifies the potential impact of disruptions from uncontrolled events and legal and regulatory requirements for the business functions

- Estimates maximum allowable downtime and acceptable levels of losses
- Estimates recovery time objectives, recovery point objectives and recovery of the critical path.

Once your BIA is complete, management should evaluate it in the context of the risk assessment process and ensure it's incorporated and tested during the business continuity planning process.

In this area, our examiners periodically find that the BCP isn't based on an effective BIA; the BIA is dated and does not reflect the bank's current operating environment; and recovery time objectives and recovery point objectives — the RTOs and RPOs — haven't been established for all areas, aren't realistic, or don't coincide with the maximum allowable downtime and acceptable levels of losses identified in the bank's policy.

In some instances, we've seen BIAs that are five years old and/or not updated to reflect the operating environment after a merger or core conversion. In addition, RTOs and RPOs haven't always been identified for each critical business function or process outlined in the BIA, and the maximum allowable downtime outlined in the BIA is less than 24 hours, yet the RTO is 36 hours.

- **Risk Assessment —** Risk assessments should ensure business processes and BIA assumptions are evaluated using multiple, realistic threat scenarios. The scenarios should consider the severity of the disaster based on the impact and probability of business disruptions.

- **Risk Management —** As members of the board and senior management, you should ensure you have adequate risk mitigation practices in place for oversight of business continuity planning, including establishing and maintaining a written, enterprise-wide BCP. Boards should approve the BCP at least annually, while senior management should ensure the BCP is distributed to employees and executed.

- **Risk Monitoring and Testing —** Risk monitoring and testing is used to validate the BCP. You should establish a testing program that:

  - Defines roles and responsibilities for testing
  - Establishes a testing schedule
  - Ensures enterprise-wide testing is completed annually
  - Ensures test results are evaluated by an independent party
  - Compares test results to the BCP to identify gaps.

In this area, our examiners periodically find testing is insufficient, hasn't been completed, or test results haven't been reported to the board. In some instances, the only testing that was done was either table-top testing or walk-through testing. These are preliminary tests and not preferred testing methods. Instead, these efforts should be supplemented by full-scale or functional drills. The BIA determines the RTOs and RPOs, which aids in determining the appropriate recovery strategy. Validation of the RTOs and RPOs is critical to ensure they're attainable.

Your business continuity planning process should be tailored to your institution. Keep in mind that without defined recovery processes or appropriate confirmation of recovery capabilities, you may have limited availability of critical systems and data in an actual disaster. This could expose your institution to financial loss and heightened legal and reputational risks.

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.

Also the Richmond Fed is hosting a Community Banking Technology Forum on September 12th. The event is in development, so be on the look-out for more information early this summer.

Resources include: *FFIEC Business Continuity Planning Booklet* and SR Letter 07-18, *FFIEC Guidance on Pandemic Planning*.

Information Technology Risk Examination Program (InTREx)

We want to update you on the enhanced information technology risk examination program, known as InTREx, for our community and regional banking organizations. Many of you received a letter explaining the program in mid-February.

The Federal Reserve System in collaboration with the FDIC and state banking agencies (through the Conference of State Bank Supervisors), began this initiative to improve consistency in the overall assessment, scoping, coverage and reporting of IT-related risks at our banks. The program also incorporates an evaluation of cybersecurity preparedness — also known as information security preparedness — into the examination process.

You may be wondering what affect this will have on upcoming IT examinations. We can assure you that this initiative does ***not*** involve new expectations for your organization. Instead, the process is designed to provide a more consistent, risk-focused IT examination approach.

What's different? Our IT examiners will call you to ask questions so we can complete an IT profile on your bank. This profile determines the scope of the examination, examiner resources and the content of the IT request list that's part of your first day letter. Also the Report of Examination will include a summary statement regarding the adequacy of your institution's cybersecurity preparedness program, including the adequacy of risk identification processes and mitigating controls.

We'll continue working with our regulatory partners to ensure consistent InTREx processes and

results. For additional information, please feel free to email Cara Mitchell, Operational Risk managing examiner, at Cara.Mitchell@rich.frb.org, or call her at (804) 697-2627.

Upcoming Banking Events at the Richmond Fed

BSA Anti-Money Laundering Conference
June 21st
The BSA Coalition's annual conference will include keynote speaker John Byrne of the Association of Certified Anti-Money Laundering Specialists, who will offer his perspectives on the Panama Papers. Law enforcement experts will share their unique perspectives, and regulators will offer an update on FinCEN's prospective beneficial ownership rules.

Community Banking Technology Forum
September 12th
Open to all banks and holding companies in the Fifth District, this IT forum will cover such topics as risks and rewards of cloud computing, disaster recovery planning, payment systems and cybersecurity.

Community Bankers Forum
November 14-15th
This forum brings together community bank leaders representing every state in our District to hear a variety of risk-focused topics and emerging issues as well as to share insights with Fed experts and one another.

Recent Speech
Lacker on Economic Leadership in an Uncertain World
In an April 12 speech, Richmond Fed President Jeffrey Lacker gave his economic outlook. He said the fact that U.S. monetary policy has diverged from policy in some other developed nations reflects the relative strength of the U.S. economy. Lacker advocated "staying the course with a gradual sequence of rate increases" in U.S. policy.

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. Active SR and CA letters are listed in reverse chronological order.

Here are recently issued guidance letters:

SR 16-9
Inactive Supervisory Guidance

SR 16-8
Off-site Review of Loan Files

SR 16-7
Interagency Guidance to Issuing Banks on Applying Customer Identification Program Requirements to Holders of Prepaid Access Cards

SR 16-6
Updates to the Expanded Examination Cycle for Certain State Member Banks and U.S. Branches and Agencies of Foreign Banking Organizations

SR 16-5
Interagency Advisory on the Use of Evaluations in Real Estate-Related Financial Transactions

SR 16-4
Relying on the Work of the Regulators of the Subsidiary Insured Depository Institution(s) of Bank Holding Companies and Savings and Loan Holding Companies with Total Consolidated Assets of Less than $50 Billion

SR 16-3
Interagency Guidance on Funds Transfer Pricing Related to Funding and Contingent Liquidity Risks

SR 16-2
Interagency Advisory on External Audits of Internationally Active U.S. Financial Institutions

SR 15-19
Federal Reserve Supervisory Assessment of Capital Planning and Positions for Large and Noncomplex Firms

SR 15-18
Federal Reserve Supervisory Assessment of Capital Planning and Positions for LISCC Firms and Large and Complex Firms

SR 15-17
Interagency Statement on Prudent Risk Management for Commercial Real Estate Lending

SR 15-16
Enhancements to the Federal Reserve System's Surveillance Program

SR 15-15
Supervisory Concerns Related to Shareholder Protection Arrangements

SR 15-14
FFIEC Information Technology Examination Handbook

SR 15-13
Supervisory Guidance on the Capital Treatment of Certain Investments in Covered Funds under the Regulatory Capital Rule and the Volcker Rule

---

For more information on Supervision News Flash subscribe here, or 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.