

# SRC Insights

FEDERAL RESERVE BANK OF PHILADELPHIA



## Sarbanes-Oxley Section 404 Compliance: What Lessons Have Been Learned?

by Eddy Hsiao, Supervising Examiner, and Joanne Branigan, Senior Examiner

The feedback from public companies, including many financial institutions, on the first year of implementation for section 404 of the Sarbanes-Oxley Act of 2002 (SOX 404) was that the requirements were unexpectedly laborious and costly. Now that the second year of SOX 404 implementation is behind most financial institutions, several questions need to be asked. Did the lessons learned from year one of SOX 404 compliance help to create a more efficient and effective compliance process in year two? Overall, are internal controls over financial reporting generally better? This article intends to address these two questions, and it will also briefly discuss the regulatory response to feedback received from the first two years of SOX 404 compliance.

### Year One: Lessons Learned

During the first year of the SOX 404 compliance process, many financial institutions may have underestimated how arduous the implementation process would be. It was especially difficult for those institutions that were already filers under section 36 of the FDI Act, because they envisioned that only minor to moderate changes would be necessary to their internal control assessment processes to satisfy SOX 404 requirements.

Consequently, some institutions encountered challenges with their compliance process, including a lack of ongoing communication with their board of directors and independent auditors, inadequate documentation and testing of controls, and insufficient allocation of resources.



continued on page 7

2

Supervision Spotlight:  
How do Examiners Assess  
Compliance Risk Management?

4

Effectively Managing  
a Business Disruption, Part II

10

Regulatory Reporting Alert

CC1

Compliance Corner

*SRC Insights* is published quarterly and is distributed to institutions supervised by the Federal Reserve Bank of Philadelphia. The current and prior issues of *SRC Insights* are available at the Federal Reserve Bank of Philadelphia's website at [www.philadelphiafed.org](http://www.philadelphiafed.org). Suggestions, comments, and requests for back issues are welcome in writing, by telephone (215-574-3760), or by e-mail ([cynthia.course@phil.frb.org](mailto:cynthia.course@phil.frb.org)). Please address all correspondence to: Cynthia L. Course, Federal Reserve Bank of Philadelphia, SRC - 7th Floor, Ten Independence Mall, Philadelphia, PA 19106-1574.

Editor .....Cynthia L. Course  
Associate Editor.....Joanne Branigan  
Designer.....Dianne Hallowell

*The views expressed in this newsletter are those of the authors and are not necessarily those of this Reserve Bank or the Federal Reserve System.*



# Supervision Spotlight

## How Do Examiners Assess Compliance Risk Management?

by Michael E. Collins, Senior Vice President

Compliance risk is defined as the current and prospective risk to earnings or capital arising from violations of, or nonconformance with, laws, rules, regulations, internal policies and procedures, or ethical standards. Effectively managing compliance risk reduces reputational and legal risk, as well as the potential for fines and civil money penalties that could result from violations.

A financial institution's overall management of risk has been part of the regulators' supervisory approach for some time. Historically, the focus has been on the traditional risk areas of credit, market, operational, liquidity, reputational, and legal risk. As the diversity and complexity of banking operations have increased over the years, bank supervisors have responded by including more in-depth assessments of compliance risk management in the examination process.

So what do examiners look for when they are conducting an assessment of compliance risk management? In general, the aim of examining compliance risk management is not to uncover one-time violations of laws and regulations, but rather to assess the adequacy of the structure and processes that management has put in place to manage the bank's compliance risk based on the nature and complexity of its operations.

During the examination scoping process, examiners review previous examination and audit findings to get an overall sense of the organization's compliance history and to identify any previous areas of concern regarding the compliance risk management program. Examiners also review the institution's compliance risk assessment, if one exists, which will help determine the level of review and testing that will be necessary during the examination.

Consistent with the other areas of risk management, supervisory expectations are the same for assessments of compliance risk management and typically include a review of the following areas:

- Board and senior management oversight
- Policies and procedures
- Internal controls
- Monitoring and reporting
- Training

The paragraphs that follow provide more information on each area as it specifically relates to what examiners look for in making their assessment of compliance risk management.

**Board and senior management oversight.** Effective compliance risk management begins with the tone set by the board of directors. A strong compliance culture incorporates all operations areas and must be well communicated so that all staff members understand their compliance responsibilities. Examiners strive to understand both the board and senior management's roles in establishing and communicating the organization's compliance culture. Examiners also determine whether these roles are clearly defined and communicated.

A compliance risk assessment serves as the foundation for risk-based policies, procedures, and internal controls. If management has created a compliance risk assessment, the examiners determine whether it properly identifies the organization's compliance risks and whether significant risks are being communicated to the board. They also determine how often the assessment is updated, how well it incorporates all of the business lines, and how it addresses new products and services.

**Policies and procedures.** Well-defined policies and procedures lay out the goals and processes of a financial institution's compliance program. Examiners review policies and procedures to determine whether they provide for adequate identification, assessment, measurement, and control of compliance risk. They also confirm whether policies and procedures are kept current and evolve as the operations of the organization evolve. Examiners also determine whether there are policies and processes in place to effectively identify and communicate compliance breaches and whether breaches are raised to the appropriate management level based on the nature of the breach.

**Internal controls.** Examiners determine whether adequate internal controls have been established to effectively manage compliance risk. This includes an assessment of reporting lines and separation of

duties, including both positive and negative incentives. Examiners also review the level and quality of compliance control testing and the manner in which control exceptions are reported to management. They also assess the procedures for tracking and resolving compliance exceptions. Examiners gain an understanding of the responsibilities of internal audit, the compliance function, and any third-party relationships to determine whether responsibilities are clearly defined and communicated.

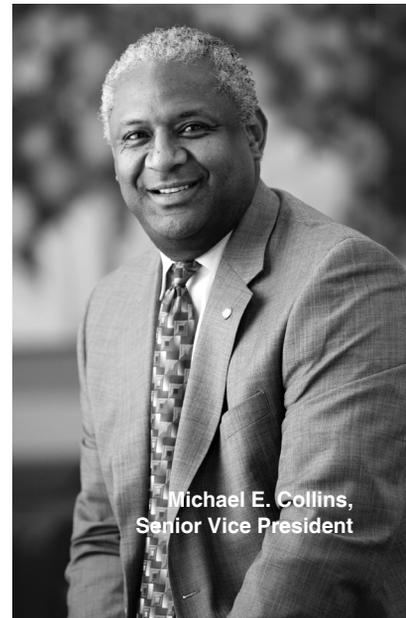
## A compliance risk assessment serves as the foundation for risk-based policies, procedures, and internal controls.

**Monitoring and reporting.** Examiners assess whether a financial institution's compliance program is designed to monitor and report on compliance concerns. Monitoring activities should reflect the size and complexity of the organization, and any monitoring reports that are generated should be thorough,

accurate, and timely. Examiners also verify that compliance monitoring information is communicated to the appropriate level within the organization.

**Training.** Examiners review a financial institution's training program to determine whether adequately communicates and promotes an understanding of the organization's compliance program. Examiners also assess whether the level of training is appropriate and effective at all levels of the organization.

Finally, examiners strive to understand that controls are in place to manage the compliance risks of an organization and to assess the overall effectiveness of a financial institution's compliance risk management program. In today's complex banking environment, it is important for financial institutions to maintain a strong compliance risk management program. □



Michael E. Collins,  
Senior Vice President

# Effectively Managing a Business Disruption: The Importance of a Business Continuity Plan, Part II

by Becky Goodwin, Assistant Examiner

After the 2005 hurricane season, many financial institutions, both those directly affected and those that were not, re-evaluated their business continuity plans in an effort to adapt to the challenges presented by the large-scale disasters of hurricanes Katrina and Rita. This article is the second of a two-part series on the topic of business continuity planning. Part I appeared in the Second Quarter 2006 issue of *SRC Insights* and outlined the essential elements of the planning process. This article will focus on best practices and lessons learned by financial institutions, specifically as a result of hurricanes Katrina and Rita.

The significance of business continuity planning was in the spotlight in the months following hurricanes Katrina and Rita. Financial institutions affected by the disaster have openly revealed the lessons learned from managing through these catastrophic events. Many financial institutions had to adjust and strengthen their existing business continuity plans (BCPs) in order to successfully respond to the needs of their community and to recover and maintain their operations.

Due to the complexity and enormity of the disaster, regulatory agencies have reinforced the importance of business continuity planning. Consequently, financial institutions and regulatory agencies continue to develop best practices to consider during the planning process. Best practices that emerge from experience serve to strengthen business continuity planning in areas that might otherwise be overlooked during the planning process.

The Hancock Holding Company (HHC), which is located in the Gulf region, endured the hurricane season of 2005. The executive management of HHC shared with us its insightful business continuity experience in managing through the disasters. In an interview on

April 6, 2006, John Hairston, EVP & COO, and Carl Chaney, EVP & CFO, detailed some key points for financial institutions to consider when establishing their BCP, including the following:

- **The importance of keeping families together.** Consider the security and mobilization of personnel (and their immediate families) required to restore and maintain critical business processes. It is important to know where all critical personnel will go during an evacuation. Consider implementing systems which will automatically inform personnel of the designated place of gathering.
- **The importance of pre-arranged contracts.** Allow for the establishment of pre-arranged, self-activating contracts with vendors who will be responsible for providing necessities in the event of a disaster, such as food, medical supplies, temporary lodging, fuel, and transportation. Keep in mind that some pre-arranged contracts may require a deposit.
- **The importance of identifying geographic locations.** Planning should take into account the geographic locations which are most critical based on the capacity to service a majority of customers from various surrounding areas.
- **The importance of volume testing.** During the testing phase of planning, the importance of volume testing is critical in determining the amount of service which allows a financial institution to operate efficiently and close to its normal capacity. Consider the capacity of voice/data telecommunications and check processing that can be maintained at the disaster recovery site.
- **The importance of a back-up communication system.** Communication is one of the most critical elements in a BCP. In the event of a widespread disaster, power outage, or technical failure, communication lines consisting of copper or



fiber can become vulnerable. Based on the size and complexity of operations, a satellite-based back-up communication system can be very effective in maintaining business processes.

- **The importance of operational readiness in the event of power failure.** Ensure that all contingent business facilities are properly wired, and require transfer switches to operate from a generator power source without compromising the security of the physical buildings. In addition, understand that the telecommunication service priority process, or TSP, between the Department of Homeland Security, the Federal Reserve, and the institution is critical to recovery.
- **The importance of senior management and board oversight.** During the initial and revision phases of planning, establish the accountability factor. Develop a rotational schedule to increase skills and promote flexibility, expand senior management involvement in the planning process, and initiate budget planning that reflects the organization's commitment to the business continuity process.

Moreover, the experiences of the Hancock Holding Company have been echoed by regulatory agencies. In February 2006, the Federal Deposit Insurance Corporation (FDIC) held a telephone conference, *Contingency Planning for Disasters and Lessons Learned from 2005 Hurricane Season*, designed to collect information relating to disaster readiness and lessons learned.<sup>1</sup> The information collected on the teleconference clearly showed that communications failed, and cash for operations and supplies was sparse. In addition, alternate sites in the path of the hurricanes could not be utilized. Furthermore, due to the vastness of the disaster, human resources could not be relied

---

<sup>1</sup> *Telephone Conference on Contingency Planning for Disasters and Lessons Learned from 2005 Hurricane Season*, February 16, 2006, is available online at <[www.fdic.gov/news/conferences/contingency\\_summary.html](http://www.fdic.gov/news/conferences/contingency_summary.html)>.

upon; employees were overwhelmingly concerned with their own safety and the safety of their relatives. As a result, best practices that emerged included improvements in the areas of communication, access to cash, alternate operation sites, and the availability of human resources—all critical components of successfully restoring and maintaining operations.

In June, the Federal Financial Institutions Examination Council (FFIEC) and the Conference of State Bank Supervisors released a booklet entitled *Lessons Learned From Hurricane Katrina: Preparing Your Institution for a Catastrophic Event*, which details the experiences shared by financial institutions and the lessons learned.<sup>2</sup>

This information indicates that a BCP should include the possibility of extensive destruction and prolonged recovery. Disaster drills should cover every critical area of operation, and provisions should be made for disruptions

in communications. Critical staff should be selected, several contacts for each critical staff person should be established, and basic supplies should be obtained to sustain the critical staff and their immediate families.

In addition, agreements should be established with vendors who will be able to provide essential supplies during a crisis. Alternate facilities should be selected, and transportation should be provided to transport critical staff and their families to the alternate site. Consideration should be given to the processing of transactions, which may not be feasible during a disaster; financial institutions may have to temporarily operate in a cash-only environment. Finally, community recovery should be considered, as institutions which are noticeably involved in the surrounding communities may reap greater benefits from doing so.

---

<sup>2</sup> *Lessons Learned from Hurricane Katrina: Preparing Your Institution for a Catastrophic Event* is available on the FFIEC's website at <[www.ffiec.gov/katrina\\_lessons.htm](http://www.ffiec.gov/katrina_lessons.htm)>.

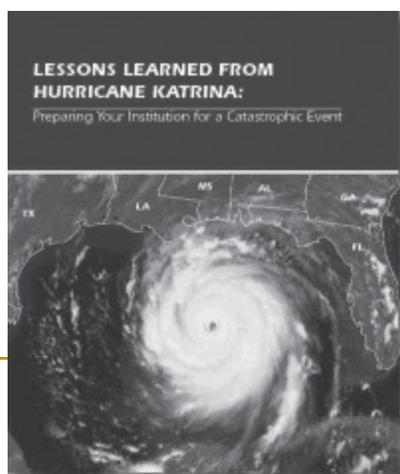
Disaster drills should cover every critical area of operation, and provisions should be made for disruptions in communications as well.

The lessons learned from the catastrophic events of hurricanes Katrina and Rita may not be applicable to all financial institutions. More importantly, business disruptions generally cannot be predicted with any certainty, but they do have the potential to impact operations significantly. Financial institutions must continue to be diligent in establishing and maintaining an effective BCP. Resiliency in responding to disasters and all business disruptions can be attributed, in large part, to effective business continuity planning. □

## Lessons Learned From Hurricane Katrina

The Federal Financial Institutions Examination Council (FFIEC) and the Conference of State Bank Supervisors have released a booklet entitled *Lessons Learned From Hurricane Katrina: Preparing Your Institution for a Catastrophic Event*. The booklet details the experiences of financial institutions in the aftermath of Hurricane Katrina and offers lessons learned that may be helpful to other institutions in considering their readiness for a catastrophic event.

The booklet is available on the FFIEC's website at <[www.ffiec.gov/katrina\\_lessons.htm](http://www.ffiec.gov/katrina_lessons.htm)>.



## SRC Hosts Directors Workshop

As part of its financial institution outreach program, the Supervision, Regulation and Credit Department (SRC) has implemented a workshop series designed to provide Third District institutions with guidance in corporate governance issues.

In June, a Directors Workshop was held in Philadelphia, and the discussion topics included fiduciary duties and responsibilities of directors and directors' knowledge of risks for financial institutions. The workshop was hosted by SRC staff and was attended by officers and directors of Third District financial institutions.

In addition to the onsite Directors Workshop, SRC plans to extend the Directors Workshop to several locations around the District and to develop a new webpage specifically for bank directors.

The Federal Reserve System also offers an on-line training course for community bank directors, which was developed to supplement an existing facilitator-led course developed by the Federal Reserve Bank of Kansas City. The course is entitled *Insights for Bank Directors: A Basic Course on Evaluating Financial Performance and Portfolio Risk*. For more information, please visit <[www.stlouisfed.org/col/director/agenda.htm](http://www.stlouisfed.org/col/director/agenda.htm)>.



# Sarbanes-Oxley Section 404 Compliance: What Lessons Have Been Learned? ...continued from page 1

These challenges produced the following negative results:

- Additional costs for outsourcing or hiring additional employees to meet compliance deadlines
- Delays in scheduled internal audit programs
- A significant number of reported material weaknesses

## Year Two: Slow Improvement

The results from year two of SOX 404 compliance were mixed. While the cost of compliance was reduced as anticipated by the Securities and Exchange Commission (SEC) and others, the decline was not as significant as anticipated. In addition, because the audit of internal controls is slowly becoming more integrated into the financial statement audit, it is often difficult to differentiate the costs of the two audits. Overall, year two did produce some improvements, but challenges remain.

**Improved communication.** Learning from the mistakes made during year one, many institutions communicated with their independent auditors early and often. Proactive discussions with their auditors provided a mutual understanding of the identified key controls, risks, and testing scope. Ongoing communication helped ensure continued agreement with regard to the sufficiency of required testing and the adequacy of remedial actions. As mentioned previously, during year one of SOX 404 compliance, some institutions incurred additional costs related to the need for additional resources to ensure compliance by the reporting deadline. Often, this was a result of the lack of early and ongoing communication with the auditors.

**Cost reduction.** As anticipated, the costs incurred for SOX 404 compliance declined in year two. A survey conducted by CRA International, Inc. reflected that smaller companies (i.e., with market capitalization between \$75 million and \$700 million) achieved a cost

savings of approximately 31 percent, and large companies (i.e., with market capitalization over \$700 million) benefited from a cost reduction of 44 percent.<sup>1</sup>

Financial institutions have indicated that they were able to achieve cost savings in year two primarily due to efficiencies gained from learning curve improvements. During year one, a considerable amount of time and effort was spent in establishing a framework to develop policies and procedures, identify controls, determine the key controls to be tested, and ascertain the adequacy of the documentation. The resources used to choose the method of identification, the mapping of controls, and the testing of procedures were greatly reduced in year two.

An analysis of some Third District institutions indicates cost savings, resulting from a reduction in professional fees paid. In year one of SOX 404 compliance, many institutions engaged consulting firms or CPA firms to assist them at various stages of the SOX 404 implementation process. These institutions were generally able to continue utilizing and enhanc-

<sup>1</sup> *Sarbanes-Oxley Section 404 Costs and Implementation Issues: Spring 2006 Survey Update*, CRA International, Inc., Washington, D.C., April 17, 2006, available online at <[www.s-oxinternalcontrolinfo.com/pdfs/CRA\\_III.pdf](http://www.s-oxinternalcontrolinfo.com/pdfs/CRA_III.pdf)>.

## Evaluating Internal Controls over Financial Reporting



ing existing processes in year two without employing external resources.

**Ongoing challenges.** The independent auditors' lack of reliance on testing and other work performed by internal staff was one of the major complaints received by the SEC after year one of SOX 404 compliance. After the year two compliance process was complete, some financial institutions commented that, while their auditors did place more reliance on the work performed by internal staff, they also required management to conduct more transactional tests in order for the auditors to obtain a comfort level. As a result of this additional testing, some potential cost savings were lost.

Integrating the audit of internal control effectiveness over financial reporting with the financial statement audit continues to be a challenge. More progress is needed in this area in order to achieve efficiencies and to reduce audit costs.

Currently, the Public Company Accounting Oversight Board (PCAOB) is considering amendments to Auditing Standard No. 2, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements (AS 2)*, which would reinforce the PCAOB's expectation that audits must be integrated and conducted in the most efficient manner while still achieving the objectives of the standard.

Another area that remains challenging is the role of the internal audit function in the SOX 404 compliance process. During the initial implementation of SOX 404, it was not uncommon for the regular audit program to be delayed or incomplete, as resources were diverted. In year two, there is still some evidence that internal audit's role remains significant, and, as a result, there is the potential for independence to be compromised. In directing the resources to be used for the SOX 404 compliance process, management must accept and maintain the responsibility for internal controls over financial reporting.

## Are Controls Generally Better?

Internal controls over financial reporting appear to have improved in 2005 based on a reduced number of institutions reporting material weaknesses in their annual reports. A review of more than 30 financial institutions' 2005 annual reports and 10Ks in the Third District revealed that only two institutions had disclosed material weaknesses in internal controls over financial reporting. The disclosed material weaknesses pertained to misreporting or misclassification of items on the statement of cash flows.

In the prior year, nine institutions had received an adverse opinion on the effectiveness of internal controls over financial reporting due to material weaknesses uncovered either by bank management or independent auditors. The primary sources of the material weaknesses disclosed last year were related to a lack of segregation of duties affecting financial reporting controls,

the ineffectiveness of controls over certain GAAP applications, and inadequate controls for and testing of information technology-related functions. One other positive sign after year two of the compliance process is that none of the nine institutions reported material weaknesses in their 2005 reports.

## Potential Regulatory Changes

Both the SEC and the PCAOB continue to take action to address the ongoing feedback from public companies related to the cost of and the difficulty with implementing SOX 404. Additional guidance was issued after year one in an effort to reduce misconceptions surrounding compliance requirements and to clarify the regulators' expectations of the implementation process.

Recently, the SEC announced a three-part plan for issuing SOX 404 guidance for management. The guidance is intended to assist management in performing a top-down, risk-based assessment of internal controls

In directing the resources to be used, management must accept and maintain the responsibility for internal controls over financial reporting.

over financial reporting. Part one of the plan, the release of a concept statement for public comment, was completed on July 11, 2006. Also as part of its plan, the SEC intends to address specific SOX 404 compliance concerns related to smaller public companies.

As mentioned previously, the PCAOB is currently considering amendments to AS 2. These amendments are part of a four-point plan announced on May 17, 2006, to improve implementation of internal control reporting requirements. The four points in the plan are listed below:

1. **Amend AS 2.** The PCAOB plans to amend the auditing standard that would direct auditors to perform their integrated audits in the most efficient manner without compromising quality.
2. **Reinforce auditor efficiency through PCAOB inspections.** Planned PCAOB 2006 inspections of registered public accounting firms will focus on the firms' efficiency in performing internal control audits.
3. **Provide guidance and education to auditors of small companies.** The PCAOB plans to facilitate opportunities for auditors of smaller public companies to obtain guidance and education on conducting internal control audits.
4. **Host PCAOB forums on auditing in the small business environment.** The PCAOB will hold eight forums in 2006 for auditors, directors, and financial officers of smaller public companies to provide them general knowledge about PCAOB issues.

### Conclusion

Financial institutions and their registered public accounting firms used the lessons learned from year one of the SOX 404 compliance process and were able to gain some efficiencies and improved effectiveness in year two. Overall, however, while some financial institutions have indicated that SOX 404 compliance costs have declined, many institutions still have reservations about the benefits of implementing SOX 404 versus the costs incurred to implement the compliance process. □

## BSA/AML Manual Revised

The Federal Financial Institutions Examination Council (FFIEC) has issued a revised *Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual*. The manual has been updated to further clarify supervisory expectations and to incorporate regulatory changes that have occurred since the original manual's release in June 2005. The revised manual reflects the ongoing efforts of the federal banking agencies and the Financial Crimes Enforcement Network (FinCEN) to provide current and consistent risk-based guidance for compliance with the Bank Secrecy Act and to safeguard operations from money laundering and terrorist financing.

As with the 2005 *FFIEC BSA/AML Examination Manual*, the revised manual does not set new standards; instead, it is a compilation of existing regulatory requirements, supervisory expectations, and sound practices in the BSA/AML area. Significant revisions and updates to the manual have been made to the following areas: risk assessment, automated clearing house transactions, trade finance activities, regulatory and supervisory guidance, emerging money laundering risks, and the manual's format.

To foster consistency, the manual includes the examination procedures that will be used by each agency's examiners and will be provided to state banking agencies. Federal Reserve examiners will begin using the examination procedures as set forth in the manual for all BSA/AML examinations beginning August 1, 2006.

The 2006 version of the manual is available on the FFIEC's website at <[www.ffiec.gov/pdf/bsa\\_aml\\_examination\\_manual2006.pdf](http://www.ffiec.gov/pdf/bsa_aml_examination_manual2006.pdf)>. With the release of the revised manual, the 2005 *FFIEC BSA/AML Examination Manual* is now retired.

# Regulatory Reporting Alert

by Eddy Hsiao, Supervising Examiner

In 2005, the FDIC exempted financial institutions with total assets of more than \$500 million but less than \$1 billion from the filing requirements of section 36 of the FDI Act (Section 36) pertaining to internal control assessments and attestations. The table below summarizes the current annual reporting requirements for section 36 compliance.

Also in 2005, the SEC granted another filing extension for compliance with section 404 of the Sarbanes-Oxley Act (Section 404) for nonaccelerated filers. The similarities in the reporting requirements of section 404 and section 36 have created some confusion for financial institutions that are subject to both laws, resulting in some section 36 reporting exceptions for the fiscal year ending December 31, 2005. This article

highlights some of the more common reporting errors to help eliminate confusion and promote understanding of the section 36 reporting requirements.

Some of the common exceptions noted during the Federal Reserve Bank of Philadelphia's (FRBP's) review of the 2005 section 36 reports submitted by required filers in the Third District are summarized in the table on the next page.

The FRBP sends an annual reminder in the first quarter to all Third District financial institutions that are required section 36 filers for the preceding calendar year. If you have questions on the section 36 reporting requirements, please contact Eddy Hsiao (eddy.hsiao@phil.frb.org) at (215) 574-3772. □

## Requirements for institutions with \$500 million or more in total assets

1. Audited comparative annual financial statements
2. A CPA's report on the audited financial statements
3. A management report that contains:
  - a. A statement of management's responsibility for:
    - Preparing the annual financial statements
    - Establishing and maintaining an adequate internal control structure over financial reporting
    - Complying with the laws and regulations relating to safety and soundness
  - b. An assessment by management of the institution's compliance with the designated laws and regulations
4. The management letter or other reports (e.g., written communication of audit findings and/or control deficiencies) issued by the financial institution's external auditor

## Requirements for institutions with \$1 billion or more in total assets

In addition to the reports noted above, institutions with \$1 billion or more in total assets must continue to include the following reports/statements in their section 36 reporting:

5. An assessment by management of the effectiveness of the internal control structure over financial reporting as of the end of the fiscal year
6. A CPA's attestation report concerning management's assessment of the institution's internal control structure over financial reporting

## Reporting Exception

## Compliance Requirement

**Omission of the statement regarding management’s responsibilities for compliance with designated safety and soundness laws and regulations and the related statement on management’s assessment of compliance.** Some institutions submitted the SOX 404 management report contained in the annual report or 10K filing to satisfy the section 36 requirements. However, the management report required by SOX 404 does not include the statement of responsibility for or the statement of compliance with designated laws and regulations.

To fully comply with section 36, the two statements regarding designated laws and regulations must be added to the SOX 404 management report or submitted as a separate report with signatures from both the chief executive officer and the chief financial officer.

**Misinterpretation of the FDIC exemption for section 36 filers with assets less than \$1 billion on the requirement of internal control assessments and attestations.** Some institutions interpreted that the exemption applied to all of the section 36 reporting requirements and, thus, did not submit any reports.

Institutions with assets of more than \$500 million but less than \$1 billion are exempt from filing the report of management’s assessment of internal controls and the related attestation by the independent accountants. They must, however, continue to submit the other required reports.

**Confusion related to the filing requirements for SOX 404 versus section 36.** Some institutions thought the extension granted by the SEC to nonaccelerated filers was applicable to section 36 filers. Hence, some small publicly-traded institutions which were subject to section 36 for the first time did not send any of the section 36 reports and assumed that they had until July 15, 2007, to comply with the reporting requirements for SOX 404 and section 36.

Depending on a financial institution’s asset size at the beginning of its fiscal year, reports must be filed accordingly (see section 36 requirements table), regardless of SOX 404 compliance status.

**Failure to submit the management letter or the written communication of audit findings issued by the independent accountants.** Some institutions that did not submit this report mistook the management report for the management letter, while others have indicated that their independent accountants did not issue a management letter. The confusion seems to be caused by the definition of “management letter.”

Regardless of the terminology used, financial institutions are required to submit to the applicable regulatory agencies any reports prepared by their independent accountants related to audit findings, reportable conditions, audit exceptions, control deficiencies, significant deficiencies, and/or material weaknesses within 15 days of receipt of the report.

## Information Technology Examination Handbook Update

The FFIEC has updated its Information Security Booklet to reflect changes in technology and mitigation strategies, as well as recent revisions to related supervisory guidance. Included in this update is expanded guidance on completing risk assessments that provides more detailed guidance on identifying information security risks

and evaluating the adequacy of controls and applicable risk management practices. The Information Security Booklet is one of 12 booklets that comprise the FFIEC’s IT Examination Handbook. The Information Security Booklet is available on the FFIEC’s website at <[www.ffiec.gov/ffiecinfobase/index.html](http://www.ffiec.gov/ffiecinfobase/index.html)>.



FEDERAL RESERVE BANK  
OF PHILADELPHIA

---

Supervision, Regulation and Credit Department  
Ten Independence Mall  
Philadelphia, PA 19106

[www.philadelphiafed.org](http://www.philadelphiafed.org)

## E-Mail Notification Service

Would you like to read *SRC Insights* and *Compliance Corner* on our website up to three weeks before they are mailed? Sign up for our e-mail notification service today at [www.philadelphiafed.org/phil\\_mailing\\_list/dsp\\_user\\_login.cfm](http://www.philadelphiafed.org/phil_mailing_list/dsp_user_login.cfm).