



# MEMORANDUM

Comptroller of the Currency  
Administrator of National Banks

MM 2004-4

Washington, DC 20219

To: All Examining Personnel

From: Emory W. Rushton, Chief National Bank Examiner

Date: October 18, 2004

Subject: Sarbanes-Oxley Act Section 404 Attestations

---

This memorandum provides additional guidance to examiners reviewing banks' compliance with section 404 of the Sarbanes-Oxley Act of 2002 (SOX). It supplements the SOX guidance in the "Internal and External Audits" booklet of the *Comptroller's Handbook*, OCC bulletins 2003-12, "Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing," and 2003-21, "Application of Recent Corporate Governance Initiatives to Non-Public Banking Organizations."

## *Background*

All public banking organizations must comply with the requirements of section 404 of SOX. Public banking organizations are defined as national banks subject to the public and periodic filing and reporting requirements of 12 CFR 11 and 12 CFR 16.20, and bank holding companies that have their securities registered with the SEC. As of May 10, 2004, the OCC regulated 36 national banks that have registered under section 12(i) of the Securities Exchange Act of 1934 and section 15(d) of the 1933 Act.<sup>1</sup>

## *Requirements of Section 404*

Section 404 requires that all public banking organizations issue a report that asserts management's responsibility over internal control, identifies the framework used to evaluate internal control, and provides an assessment of the effectiveness of the organization's internal control over financial reporting. Further, it requires that the company's external auditor attest to, and report on, management's assessment of internal control. A copy of the attestation report must be filed along with the banking organization's annual report on Form 10K with either the OCC or SEC, as appropriate, beginning with the first fiscal year ending on or after November 15, 2004.<sup>2</sup>

---

<sup>1</sup> To obtain a current list of registered national banks, contact the Securities & Corporate Practices Division.

<sup>2</sup> All accelerated filers must comply by this date. Nonaccelerated filers must comply in the first fiscal year ending on or after July 15, 2005. An accelerated filer, as defined in Exchange Act Rule 12b-2, is generally a U.S. company that has equity market capitalization over \$75 million and has filed at least one annual report.

### *Registered National Banks*

For the national banks that have a class of securities registered with the OCC under 12 CFR 11 or 12 CFR 16, examiners are directly responsible for assessing compliance with the requirements of SOX. In these banks, if the review of the overall compliance program, including section 404 supporting documentation, reveals any significant weaknesses, the examiner should discuss the matter with bank management and the board and include them in a “matters requiring attention” in the report of examination and, if appropriate, cite a violation of law on the specific section of SOX at the bank level.

### *Registered Holding Companies*

For national banks that are subsidiaries of holding companies registered with the U.S. Securities and Exchange Commission (SEC), the OCC is not directly responsible for assessing compliance with SOX, since compliance is assessed at the holding company level. However, for these institutions, examiners should gain sufficient understanding of the holding company’s overall SOX compliance program to determine any impact on the risk profile of the national bank. The bank’s reputation risk may increase if full compliance with SOX is not achieved at the holding company level. The scope of the supervisory activities required to assess this risk should be based on the institution’s size and complexity. If the review of the overall compliance program reveals any significant weaknesses, the examiner should discuss them with bank management and the board and include them as “matters requiring attention” in the report of examination. Violations of law regarding any section of SOX at the holding company level should not be cited at the bank level. Such violations or concerns should be forwarded to the bank’s holding company regulator. Examiners should coordinate such communications with their supervisory office.

### *Tools for Evaluating Section 404 Compliance*

#### Best Practices

A recently completed limited horizontal review of the section 404 programs in large banks identified some best practices that banks have used as part of their program implementation activities. Examiners might find these practices helpful when reviewing and assessing the current status of any public banking organization’s program. These best practices included:

- Using standardized format throughout the institution for the process and control documentation.
- Using both quantitative and qualitative factors when deciding what controls to document.
- Having strong quality assurance throughout the process.
- Having good management information systems.
- Appropriately overlapping the section 404 assessment process with the existing assessment process for 12 CFR 363.

- Having proactive oversight by a committee consisting of both management and board representation.
- Establishing a centralized monitoring system for any control gaps that are identified (similar to an audit exception tracking system) and requiring that all remediation be completed by year-end.

Examiners should evaluate each institution's section 404 program on its own merits, given the institution's size and complexity, recognizing that a program lacking any of the above practices may still be appropriate for an individual institution.

### Practical Section 404 Implementation Issues

Examiners may also find the following information from the large bank horizontal review useful in assessing a bank's overall progress in achieving full compliance with the requirements of section 404:

- Most banks found that they underestimated the time needed for the section 404 process.
- Some banks are experiencing shortages in information technology expertise needed for the process.
- Most banks are experiencing a negative impact on the current level of internal audit coverage, but the overall assessment will benefit the internal audit program in future years.
- Most banks had estimated the completion of this year's documentation phase by late July 2004.
- On average, bank 404 processes are documenting controls for over 80 percent of the balance sheet/income statement general ledger accounts.
- Some testing phases are extending as late as 1<sup>st</sup> quarter 2005, since the external auditors will not start their review then. However, for December 31, 2004 attestations, all remediation efforts must still be completed by year-end.
- External audit firms are having a significant impact on the documentation and quality assurance parts of the process since they are now being held to a higher auditing standard by the Public Company Accounting Oversight Board (PCAOB).<sup>3</sup>

### Questions to Consider:

The following questions can be used by examiners in discussions with bank management and to assist them in determining the appropriateness of the process:

- Who has been assigned the responsibility for the overall process?
- Where is the bank in the process?
- How is account significance being determined? Are both quantitative and qualitative factors being used?

---

<sup>3</sup> For additional information regarding the responsibilities of independent auditors, see PCAOB Auditing Standard No. 2, "An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements" ([www.pcaobus.org](http://www.pcaobus.org)).

- How extensive are quality assurance efforts? Is there a process in place for reviewing the documentation prior to the start of testing?
- What are the time frames for testing and when will the results be handed off to the external auditors?
- How are they determining what level of testing is needed? Does the level of testing seem appropriate? How are any identified control gaps being monitored? What is the process/system for any remediation that will be required?
- What is the current 404 staffing? Is the staffing adequate? What are plans for future staffing? What is the future role of internal audit in the process?
- What is the role of the external auditor in the process? (The bank should have ongoing communication with the external auditor throughout the process since the external auditor has the ultimate responsibility for attesting to the controls.)

#### *Additional Section 404 Questions and Answers*

##### Are the internal control attestations for section 404 and 12 CFR 363 (FDICIA) different?

Yes. In addition to the SOX internal control attestation requirements on public banking organizations noted above, national banks with assets greater than \$500 million must comply with the attestation requirements of 12 CFR 363, Annual Independent Audits and Reporting Requirements.<sup>4</sup> While section 404 and 12 CFR 363 both require attestations regarding internal control, some differences exist. For public banking organizations that must comply with both section 404 and 12 CFR 363, they have the option of issuing two separate reports or one report that includes all of the following:<sup>5</sup>

- A statement of the management’s responsibility for preparing the registrant’s annual financial statements, for establishing and maintaining adequate internal control over financial reporting, and for ensuring the institution’s compliance with laws and regulations relating to safety and soundness.
- A statement identifying the framework used by management to evaluate the effectiveness of the registrant’s internal control over financial reporting.
- Management’s assessment of the effectiveness of the registrant’s internal control over financial reporting as of the end of the registrant’s most recent fiscal year. The assessment must include a statement as to whether management has concluded that the registrant’s internal control over financial reporting is effective, and whether the institution has complied with the designated safety and soundness laws and regulations during the fiscal year. This

---

<sup>4</sup> Part 363 establishes requirements for independent financial statement audits; timing, contents, and types of management and auditor reporting; and the board of director’s audit committee structure and responsibilities.

<sup>5</sup> From the AICPA’s Audit Risk Alert, “Bank, Credit Union, and Other Depository and Lending Institution Industry Developments – 2003/2004” ([www.aicpa.org](http://www.aicpa.org)). If two reports are issued, refer to the Part 363 Annual Report Worksheet in the “Internal and External Audits Handbook” and the above audit risk alert for further guidance on the specific requirements for each report.

statement must disclose any material weakness in the registrant's internal control over financial reporting identified by management.

- A statement that the registered public accounting firm that audited the financial statements included in the registrant's annual report has issued an attestation report on management's assessment of the registrant's internal control over financial reporting.

Can the reporting requirements of 12 CFR 363 be satisfied at the holding company level?

Yes. The requirement for audited financial statements, audit report, management report, and independent public accountant's report on internal controls over financial reporting may be satisfied at the holding company level for any bank with assets between \$500 million and \$5 billion. Banks larger than \$5 billion can also submit at the holding company level if they have an assigned CAMELS composite rating of 1 or 2. Banks larger than \$5 billion rated 3 or worse may submit holding company financial statements and audit reports, but all other reports mentioned above must be at the bank level.

Are there plans to modify 12 CFR 363?

There is currently an interagency working group comparing the requirements of part 363 to those in Sarbanes-Oxley. However, if the rule is revised, it will not be effective until some time after December 31, 2004.

What is the appropriate structure for an internal control assessment program?

All effective internal control assessment programs will have the following components, although they may be either formal or informal depending on the size and complexity of the bank:

- Assessment
- Documentation
- Testing
- Remediation
- Compliance

What is the minimum level of supervisory activities examiners should complete to test compliance with section 404?

Using the 12 CFR 363 objectives in the "Internal and External Audits" and "Internal Control" booklets of the *Comptroller's Handbook* as a guide, examiners should complete sufficient supervisory activities to determine the effectiveness of the internal control assessment program, based on the review of the five components noted above. The depth and scope of the activities will vary based on the size and complexity of the bank.

What should examiners focus on when reviewing the effectiveness of internal control assessment programs?

Examiners should focus their supervisory reviews on assessing the appropriateness of the overall process. If examiners determine that the scope of their supervisory activities should include reviewing and validating a sample of section 404 documentation or testing, they should select areas where internal audit or the OCC has identified significant weaknesses. Examiners should also target for supervisory follow-up any areas where the bank's assessment identifies any gaps or shortfalls in internal controls.

However, in determining the effectiveness of an institution's internal control assessment program, there is no "one size fits all" model. The SEC has stated that the methods of conducting evaluations of internal control over financial reporting will, and should, vary from company to company.<sup>6</sup> Examiners should consider the size and complexity of the organization when assessing the program's effectiveness, as they do when reviewing national bank compliance with 12 CFR 363 as outlined in the "Internal and External Audits" booklet. Examiners should also determine whether the institution has communicated with its external auditors to ensure that the bank's program meets the auditor's requirements and will not hinder the auditor's ability to attest to management's assessment of internal controls.

*Additional Information*

Examiners should be aware that the points above are provided for informational purposes only, and if their findings differ, it does not mean the institution will not achieve full compliance with section 404. Examiners with additional questions on this topic should contact Amy Hundley, policy analyst in Operational Risk Policy at (202) 874-4849, or Karen Kwilosz, the division's director at (202) 874-9457.

---

<sup>6</sup> From the SEC Release No. 33-8238, "Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports," issued June 5, 2003 ([www.sec.gov](http://www.sec.gov)).