

1831a(f) to hold equity securities may continue to establish new subsidiaries to engage in that investment activity.

(3) *Relief from conditions.* Any state nonmember bank that meets the requirements of paragraph (g)(1) of this section or that is subject to section 46(b) of the Federal Deposit Insurance Act (12 U.S.C. 1831w(b)) may submit an application in compliance with §303.121 of this chapter and seek the consent of the FDIC under the procedure in §303.122(b) of this chapter for modification of any conditions or restrictions the FDIC previously imposed in connection with a section 24 order or regulation approving the activity.

(4) *New financial subsidiaries.* Notwithstanding subpart A of this part 362, an insured state bank may not, on or after November 12, 1999, acquire control of, or acquire an interest in, a financial subsidiary that engages in activities as principal or commences any new activity under section 46(a) of the Federal Deposit Insurance Act (12 U.S.C. 1831w) other than as provided in this section.

PART 363—ANNUAL INDEPENDENT AUDITS AND REPORTING REQUIREMENTS

Sec.

363.0 OMB control number.

363.1 Scope and definitions.

363.2 Annual reporting requirements.

363.3 Independent public accountant.

363.4 Filing and notice requirements.

363.5 Audit committees.

APPENDIX A TO PART 363—GUIDELINES AND INTERPRETATIONS

APPENDIX B TO PART 363—ILLUSTRATIVE MANAGEMENT REPORTS

AUTHORITY: 12 U.S.C. 1831m.

SOURCE: 74 FR 35745, July 20, 2009, unless otherwise noted.

§ 363.0 OMB control number.

The information collection requirements in this part have been approved by the Office of Management and Budget under OMB control number 3064–0113.

§ 363.1 Scope and definitions.

(a) *Applicability.* This part applies to any insured depository institution with respect to any fiscal year in which its consolidated total assets as of the beginning of such fiscal year are \$500 mil-

lion or more. The requirements specified in this part are in addition to any other statutory and regulatory requirements otherwise applicable to an insured depository institution.

(b) *Compliance by subsidiaries of holding companies.* (1) For an insured depository institution that is a subsidiary of a holding company, the audited financial statements requirement of §363.2(a) may be satisfied:

(i) For fiscal years ending on or before June 14, 2010, by audited consolidated financial statements of the top-tier or any mid-tier holding company.

(ii) For fiscal years ending on or after June 15, 2010, by audited consolidated financial statements of the top-tier or any mid-tier holding company provided that the consolidated total assets of the insured depository institution (or the consolidated total assets of all of the holding company's insured depository institution subsidiaries, regardless of size, if the holding company owns or controls more than one insured depository institution) comprise 75 percent or more of the consolidated total assets of this top-tier or mid-tier holding company as of the beginning of its fiscal year.

(2) The other requirements of this part for an insured depository institution that is a subsidiary of a holding company may be satisfied by the top-tier or any mid-tier holding company if the insured depository institution meets the criterion specified in §363.1(b)(1) and if:

(i) The services and functions comparable to those required of the insured depository institution by this part are provided at this top-tier or mid-tier holding company level; and

(ii) The insured depository institution has as of the beginning of its fiscal year:

(A) Total assets of less than \$5 billion; or

(B) Total assets of \$5 billion or more and a composite CAMELS rating of 1 or 2.

(3) The appropriate Federal banking agency may revoke the exception in paragraph (b)(2) of this section for any institution with total assets in excess of \$9 billion for any period of time during which the appropriate Federal

Federal Deposit Insurance Corporation

§ 363.2

banking agency determines that the institution's exemption would create a significant risk to the Deposit Insurance Fund.

(c) *Financial reporting.* For purposes of the management report requirement of § 363.2(b) and the internal control reporting requirement of § 363.3(b), "financial reporting," at a minimum, includes both financial statements prepared in accordance with generally accepted accounting principles for the insured depository institution or its holding company and financial statements prepared for regulatory reporting purposes. For recognition and measurement purposes, financial statements prepared for regulatory reporting purposes shall conform to generally accepted accounting principles and section 37 of the Federal Deposit Insurance Act.

(d) *Definitions.* For purposes of this part, the following definitions apply:

(1) *AICPA* means the American Institute of Certified Public Accountants.

(2) *GAAP* means generally accepted accounting principles.

(3) *PCAOB* means the Public Company Accounting Oversight Board.

(4) *Public company* means an insured depository institution or other company that has a class of securities registered with the U.S. Securities and Exchange Commission or the appropriate Federal banking agency under Section 12 of the Securities Exchange Act of 1934 and *nonpublic company* means an insured depository institution or other company that does not meet the definition of a *public company*.

(5) *SEC* means the U.S. Securities and Exchange Commission.

(6) *SOX* means the Sarbanes-Oxley Act of 2002.

§ 363.2 Annual reporting requirements.

(a) *Audited financial statements.* Each insured depository institution shall prepare annual financial statements in accordance with GAAP, which shall be audited by an independent public accountant. The annual financial statements must reflect all material correcting adjustments necessary to conform with GAAP that were identified by the independent public accountant.

(b) *Management report.* Each insured depository institution annually shall

prepare, as of the end of the institution's most recent fiscal year, a management report that must contain the following:

(1) A statement of management's responsibilities for preparing the institution's annual financial statements, for establishing and maintaining an adequate internal control structure and procedures for financial reporting, and for complying with laws and regulations relating to safety and soundness that are designated by the FDIC and the appropriate Federal banking agency;

(2) An assessment by management of the insured depository institution's compliance with such laws and regulations during such fiscal year. The assessment must state management's conclusion as to whether the insured depository institution has complied with the designated safety and soundness laws and regulations during the fiscal year and disclose any noncompliance with these laws and regulations; and

(3) For an insured depository institution with consolidated total assets of \$1 billion or more as of the beginning of such fiscal year, an assessment by management of the effectiveness of such internal control structure and procedures as of the end of such fiscal year that must include the following:

(i) A statement identifying the internal control framework¹⁴ used by management to evaluate the effectiveness of the insured depository institution's internal control over financial reporting;

(ii) A statement that the assessment included controls over the preparation of regulatory financial statements in accordance with regulatory reporting instructions including identification of such regulatory reporting instructions; and

¹⁴For example, in the United States, the Committee of Sponsoring Organizations (COSO) of the Treadway Commission has published *Internal Control—Integrated Framework*, including an addendum on safeguarding assets. Known as the COSO report, this publication provides a suitable and available framework for purposes of management's assessment.

§ 363.3

(iii) A statement expressing management's conclusion as to whether the insured depository institution's internal control over financial reporting is effective as of the end of its fiscal year. Management must disclose all material weaknesses in internal control over financial reporting, if any, that it has identified that have not been remediated prior to the insured depository institution's fiscal year-end. Management is precluded from concluding that the institution's internal control over financial reporting is effective if there are one or more material weaknesses.

(c) *Management report signatures.* Subject to the criteria specified in § 363.1(b):

(1) If the audited financial statements requirement specified in § 363.2(a) is satisfied at the insured depository institution level and the management report requirement specified in § 363.2(b) is satisfied in its entirety at the insured depository institution level, the management report must be signed by the chief executive officer and the chief accounting officer or chief financial officer of the insured depository institution;

(2) If the audited financial statements requirement specified in § 363.2(a) is satisfied at the holding company level and the management report requirement specified in § 363.2(b) is satisfied in its entirety at the holding company level, the management report must be signed by the chief executive officer and the chief accounting officer or chief financial officer of the holding company; and

(3) If the audited financial statements requirement specified in § 363.2(a) is satisfied at the holding company level and (i) the management report requirement specified in § 363.2(b) is satisfied in its entirety at the insured depository institution level or (ii) one or more of the components of the management report specified in § 363.2(b) is satisfied at the holding company level and the remaining components of the management report are satisfied at the insured depository institution level, the management report must be signed by the chief executive officers and the chief accounting officers or chief financial officers of both the holding company and the insured

12 CFR Ch. III (1–1–13 Edition)

depository institution and the management report must clearly indicate the level (institution or holding company) at which each of its components is being satisfied.

§ 363.3 Independent public accountant.

(a) *Annual audit of financial statements.* Each insured depository institution shall engage an independent public accountant to audit and report on its annual financial statements in accordance with generally accepted auditing standards or the PCAOB's auditing standards, if applicable, and section 37 of the Federal Deposit Insurance Act (12 U.S.C. 1831n). The scope of the audit engagement shall be sufficient to permit such accountant to determine and report whether the financial statements are presented fairly and in accordance with GAAP.

(b) *Internal control over financial reporting.* For each insured depository institution with total assets of \$1 billion or more at the beginning of the institution's fiscal year, the independent public accountant who audits the institution's financial statements shall examine, attest to, and report separately on the assertion of management concerning the effectiveness of the institution's internal control structure and procedures for financial reporting. The attestation and report shall be made in accordance with generally accepted standards for attestation engagements or the PCAOB's auditing standards, if applicable. The accountant's report must not be dated prior to the date of the management report and management's assessment of the effectiveness of internal control over financial reporting. Notwithstanding the requirements set forth in applicable professional standards, the accountant's report must include the following:

(1) A statement identifying the internal control framework used by the independent public accountant, which must be the same as the internal control framework used by management, to evaluate the effectiveness of the insured depository institution's internal control over financial reporting;

(2) A statement that the independent public accountant's evaluation included controls over the preparation of

Federal Deposit Insurance Corporation

§ 363.3

regulatory financial statements in accordance with regulatory reporting instructions including identification of such regulatory reporting instructions; and

(3) A statement expressing the independent public accountant's conclusion as to whether the insured depository institution's internal control over financial reporting is effective as of the end of its fiscal year. The report must disclose all material weaknesses in internal control over financial reporting that the independent public accountant has identified that have not been remediated prior to the insured depository institution's fiscal year-end. The independent public accountant is precluded from concluding that the insured depository institution's internal control over financial reporting is effective if there are one or more material weaknesses.

(c) *Notice by accountant of termination of services.* An independent public accountant performing an audit under this part who ceases to be the accountant for an insured depository institution shall notify the FDIC, the appropriate Federal banking agency, and any appropriate State bank supervisor in writing of such termination within 15 days after the occurrence of such event, and set forth in reasonable detail the reasons for such termination. The written notice shall be filed at the place identified in §363.4(f).

(d) *Communications with audit committee.* In addition to the requirements for communications with audit committees set forth in applicable professional standards, the independent public accountant must report the following on a timely basis to the audit committee:

(1) All critical accounting policies and practices to be used by the insured depository institution,

(2) All alternative accounting treatments within GAAP for policies and practices related to material items that the independent public accountant has discussed with management, including the ramifications of the use of such alternative disclosures and treatments, and the treatment preferred by the independent public accountant, and

(3) Other written communications the independent public accountant has

provided to management, such as a management letter or schedule of unadjusted differences.

(e) *Retention of working papers.* The independent public accountant must retain the working papers related to the audit of the insured depository institution's financial statements and, if applicable, the evaluation of the institution's internal control over financial reporting for seven years from the report release date, unless a longer period of time is required by law.

(f) *Independence.* The independent public accountant must comply with the independence standards and interpretations of the AICPA, the SEC, and the PCAOB. To the extent that any of the rules within any one of these independence standards (AICPA, SEC, and PCAOB) is more or less restrictive than the corresponding rule in the other independence standards, the independent public accountant must comply with the more restrictive rule.

(g) *Peer reviews and inspection reports.* (1) Prior to commencing any services for an insured depository institution under this part, the independent public accountant must have received a peer review, or be enrolled in a peer review program, that meets acceptable guidelines. Acceptable peer reviews include peer reviews performed in accordance with the AICPA's Peer Review Standards and inspections conducted by the PCAOB.

(2) Within 15 days of receiving notification that a peer review has been accepted or a PCAOB inspection report has been issued, or before commencing any audit under this part, whichever is earlier, the independent public accountant must file two copies of the most recent peer review report and the public portion of the most recent PCAOB inspection report, if any, accompanied by any letters of comments, response, and acceptance, with the FDIC, Accounting and Securities Disclosure Section, 550 17th Street, NW., Washington, DC 20429, if the report has not already been filed. The peer review reports and the public portions of the PCAOB inspection reports will be made available for public inspection by the FDIC.

(3) Within 15 days of the PCAOB making public a previously nonpublic

§ 363.4

12 CFR Ch. III (1–13 Edition)

portion of an inspection report, the independent public accountant must file two copies of the previously nonpublic portion of the inspection report with the FDIC, Accounting and Securities Disclosure Section, 550 17th Street, NW., Washington, DC 20429. Such previously nonpublic portion of the PCAOB inspection report will be made available for public inspection by the FDIC.

§ 363.4 Filing and notice requirements.

(a) *Part 363 Annual Report.* (1) Each insured depository institution shall file with each of the FDIC, the appropriate Federal banking agency, and any appropriate State bank supervisor, two copies of its Part 363 Annual Report. A Part 363 Annual Report must contain audited comparative annual financial statements, the independent public accountant's report thereon, a management report, and, if applicable, the independent public accountant's attestation report on management's assessment concerning the institution's internal control structure and procedures for financial reporting as required by §§ 363.2(a), 363.3(a), 363.2(b), and 363.3(b), respectively.

(2) Subject to the criteria specified in § 363.1(b), each insured depository institution with consolidated total assets of less than \$1 billion as of the beginning of its fiscal year that is required to file, or whose parent holding company is required to file, management's assessment of the effectiveness of internal control over financial reporting with the SEC or the appropriate Federal banking agency in accordance with section 404 of SOX must submit a copy of such assessment to the FDIC, the appropriate Federal banking agency, and any appropriate State bank supervisor with its Part 363 Annual Report as additional information. This assessment will not be considered part of the institution's Part 363 Annual Report.

(3)(i) Each insured depository institution that is neither a public company nor a subsidiary of a public company that meets the criterion specified in § 363.1(b)(1) shall file its Part 363 Annual Report within 120 days after the end of its fiscal year. (ii) Each insured depository institution that is a public

company or a subsidiary of public company that meets the criterion specified in § 363.1(b)(1) shall file its Part 363 Annual Report within 90 days after the end of its fiscal year.

(b) *Public availability.* Except for the annual report in paragraph (a)(1) of this section and the peer reviews and inspection reports in § 363.3(g), which shall be available for public inspection, the FDIC has determined that all other reports and notifications required by this part are exempt from public disclosure by the FDIC.

(c) *Independent public accountant's letters and reports.* Except for the independent public accountant's reports that are included in its Part 363 Annual Report, each insured depository institution shall file with the FDIC, the appropriate Federal banking agency, and any appropriate State bank supervisor, a copy of any management letter or other report issued by its independent public accountant with respect to such institution and the services provided by such accountant pursuant to this part within 15 days after receipt. Such reports include, but are not limited to:

(1) Any written communication regarding matters that are required to be communicated to the audit committee (for example, critical accounting policies, alternative accounting treatments discussed with management, and any schedule of unadjusted differences),

(2) Any written communication of significant deficiencies and material weaknesses in internal control required by the AICPA's or the PCAOB's auditing standards;

(3) For institutions with total assets of less than \$1 billion as of the beginning of their fiscal year that are public companies or subsidiaries of public companies that meet the criterion specified in § 363.1(b)(1), any independent public accountant's report on the audit of internal control over financial reporting required by section 404 of SOX and the PCAOB's auditing standards; and

(4) For all institutions that are public companies or subsidiaries of public companies that meet the criterion specified in § 363.1(b)(1), any independent public accountant's written communication of all deficiencies in

Federal Deposit Insurance Corporation

§ 363.5

internal control over financial reporting that are of a lesser magnitude than significant deficiencies required by the PCAOB's auditing standards.

(d) *Notice of engagement or change of accountants.* Each insured depository institution shall provide, within 15 days after the occurrence of any such event, written notice to the FDIC, the appropriate Federal banking agency, and any appropriate State bank supervisor of the engagement of an independent public accountant, or the resignation or dismissal of the independent public accountant previously engaged. The notice shall include a statement of the reasons for any such resignation or dismissal in reasonable detail.

(e) *Notification of late filing.* No extensions of time for filing reports required by § 363.4 shall be granted. An insured depository institution that is unable to timely file all or any portion of its Part 363 Annual Report or any other report or notice required by § 363.4 shall submit a written notice of late filing to the FDIC, the appropriate Federal banking agency, and any appropriate State bank supervisor. The notice shall disclose the institution's inability to timely file all or specified portions of its Part 363 Annual Report or any other report or notice and the reasons therefore in reasonable detail. The late filing notice shall also state the date by which the report or notice will be filed. The written notice shall be filed on or before the deadline for filing the Part 363 Annual Report or any other report or notice, as appropriate.

(f) *Place for filing.* The Part 363 Annual Report, any written notification of late filing, and any other report or notice required by § 363.4 should be filed as follows:

(1) *FDIC:* Appropriate FDIC Regional or Area Office (Division of Supervision and Consumer Protection), *i.e.*, the FDIC regional or area office in the FDIC region or area that is responsible for monitoring the institution or, in the case of a subsidiary institution of a holding company, the consolidated company. A filing made on behalf of several covered institutions owned by the same parent holding company should be accompanied by a trans-

mittal letter identifying all of the institutions covered.

(2) *Office of the Comptroller of the Currency (OCC):* Appropriate OCC Supervisory Office.

(3) *Federal Reserve:* Appropriate Federal Reserve Bank.

(4) *Office of Thrift Supervision (OTS):* Appropriate OTS District Office.

(5) *State bank supervisor:* The filing office of the appropriate State bank supervisor.

§ 363.5 Audit committees.

(a) *Composition and duties.* Each insured depository institution shall establish an audit committee of its board of directors, the composition of which complies with paragraphs (a)(1), (2), and (3) of this section. The duties of the audit committee shall include the appointment, compensation, and oversight of the independent public accountant who performs services required under this part, and reviewing with management and the independent public accountant the basis for the reports issued under this part.

(1) Each insured depository institution with total assets of \$1 billion or more as of the beginning of its fiscal year shall establish an independent audit committee of its board of directors, the members of which shall be outside directors who are independent of management of the institution.

(2) Each insured depository institution with total assets of \$500 million or more but less than \$1 billion as of the beginning of its fiscal year shall establish an audit committee of its board of directors, the members of which shall be outside directors, the majority of whom shall be independent of management of the institution. The appropriate Federal banking agency may, by order or regulation, permit the audit committee of such an insured depository institution to be made up of less than a majority of outside directors who are independent of management, if the agency determines that the institution has encountered hardships in retaining and recruiting a sufficient number of competent outside directors to serve on the audit committee of the institution.

(3) An outside director is a director who is not, and within the preceding

fiscal year has not been, an officer or employee of the institution or any affiliate of the institution.

(b) *Committees of large institutions.* The audit committee of any insured depository institution with total assets of more than \$3 billion as of the beginning of its fiscal year shall include members with banking or related financial management expertise, have access to its own outside counsel, and not include any large customers of the institution. If a large institution is a subsidiary of a holding company and relies on the audit committee of the holding company to comply with this rule, the holding company's audit committee shall not include any members who are large customers of the subsidiary institution.

(c) *Independent public accountant engagement letters.* (1) In performing its duties with respect to the appointment of the institution's independent public accountant, the audit committee shall ensure that engagement letters and any related agreements with the independent public accountant for services to be performed under this part do not contain any limitation of liability provisions that:

(i) Indemnify the independent public accountant against claims made by third parties;

(ii) Hold harmless or release the independent public accountant from liability for claims or potential claims that might be asserted by the client insured depository institution, other than claims for punitive damages; or

(iii) Limit the remedies available to the client insured depository institution.

(2) Alternative dispute resolution agreements and jury trial waiver provisions are not precluded from engagement letters provided that they do not incorporate any limitation of liability provisions set forth in paragraph (c)(1) of this section.

APPENDIX A TO PART 363—GUIDELINES AND INTERPRETATIONS

TABLE OF CONTENTS

Introduction
 Scope of Rule and Definitions (§363.1)
 1. Measuring Total Assets
 2. Insured Branches of Foreign Banks

3. Compliance by Holding Company Subsidiaries
 4. Comparable Services and Functions
 4A. Financial Reporting
 Annual Reporting Requirements (§363.2)
 5. Annual Financial Statements
 5A. Institutions Merged out of Existence
 6. Holding Company Statements
 7. Insured Branches of Foreign Banks
 7A. Compliance with Designated Laws and Regulations
 8. Management Report
 8A. Management's Reports on Internal Control over Financial Reporting under Part 363 and Section 404 of SOX
 8B. Internal Control Reports and Part 363 Annual Reports for Acquired Businesses
 8C. Management's Disclosure of Non-compliance with the Designated Laws and Regulations
 9. Safeguarding of Assets
 10. Standards for Internal Control
 11. Service Organizations
 12. Reserved
 Role of Independent Public Accountant (§363.3)
 13. General Qualifications
 14. Reserved
 15. Peer Review Guidelines
 16. Reserved
 17. Information to be Provided to the Independent Public Accountant
 18. Attestation Report and Management Letters
 18A. Internal Control Attestation Standards for Independent Auditors
 19. Reviews with Audit Committee and Management
 20. Notice of Termination
 21. Reliance on Internal Auditors
 Filing and Notice Requirements (§363.4)
 22. Reserved
 23. Notification of Late Filing
 24. Public Availability
 25. Reserved
 26. Notices Concerning Accountants
 Audit Committees (§363.5)
 27. Composition
 28. "Independent of Management" Considerations
 29. Reserved
 30. Holding Company Audit Committees
 31. Duties
 32. Banking or Related Financial Management Expertise
 33. Large Customers
 34. Access to Counsel
 35. Transition Period for Forming and Restructuring Audit Committees
 Other
 36. Modifications of Guidelines

INTRODUCTION

Congress added section 36, "Early Identification of Needed Improvements in Financial Management" (section 36), to the Federal Deposit Insurance Act (FDI Act) in 1991.

The FDIC Board of Directors adopted 12 CFR part 363 of its rules and regulations (the Rule) to implement those provisions of section 36 that require rulemaking. The FDIC also approved these "Guidelines and Interpretations" (the Guidelines) and directed that they be published with the Rule to facilitate a better understanding of, and full compliance with, the provisions of section 36.

Although not contained in the Rule itself, some of the guidance offered restates or refers to statutory requirements of section 36 and is therefore mandatory. If that is the case, the statutory provision is cited.

Furthermore, upon adopting the Rule, the FDIC reiterated its belief that every insured depository institution, regardless of its size or charter, should have an annual audit of its financial statements performed by an independent public accountant, and should establish an audit committee comprised entirely of outside directors.

The following Guidelines reflect the views of the FDIC concerning the interpretation of section 36. The Guidelines are intended to assist insured depository institutions (institutions), their boards of directors, and their advisors, including their independent public accountants and legal counsel, and to clarify section 36 and the Rule. It is recognized that reliance on the Guidelines may result in compliance with section 36 and the Rule which may vary from institution to institution. Terms which are not explained in the Guidelines have the meanings given them in the Rule, the FDI Act, or professional accounting and auditing literature.

SCOPE OF RULE AND DEFINITIONS (§363.1)

1. *Measuring Total Assets.* To determine whether this part applies, an institution should use total assets as reported on its most recent Report of Condition (Call Report) or Thrift Financial Report (TFR), the date of which coincides with the end of its preceding fiscal year. If its fiscal year ends on a date other than the end of a calendar quarter, it should use its Call Report or TFR for the quarter end immediately preceding the end of its fiscal year.

2. *Insured Branches of Foreign Banks.* Unlike other institutions, insured branches of foreign banks are not separately incorporated or capitalized. To determine whether this part applies, an insured branch should measure claims on non-related parties reported on its Report of Assets and Liabilities of U.S. Branches and Agencies of Foreign Banks (form FFIEC 002).

3. *Compliance by Holding Company Subsidiaries.* Audited consolidated financial statements and other reports or notices required by this part that are submitted by a holding company for any subsidiary institution should be accompanied by a cover letter identifying all subsidiary institutions subject to part 363 that are included in the hold-

ing company's submission. When submitting a Part 363 Annual Report, the cover letter should identify all subsidiary institutions subject to part 363 included in the consolidated financial statements and state whether the other annual report requirements (*i.e.*, management's statement of responsibilities, management's assessment of compliance with designated safety and soundness laws and regulations, and, if applicable, management's assessment of the effectiveness of internal control over financial reporting and the independent public accountant's attestation report on management's internal control assessment) are being satisfied for these institutions at the holding company level or at the institution level. An institution filing holding company consolidated financial statements as permitted by §363.1(b)(1) also may report on changes in its independent public accountant on a holding company basis. An institution that does not meet the criteria in §363.1(b)(2) must satisfy the remaining provisions of this part on an individual institution basis and maintain its own audit committee. Subject to the criteria in §§363.1(b)(1) and (2), a multi-tiered holding company may satisfy all of the requirements of this part at the top-tier or any mid-tier holding company level.

4. *Comparable Services and Functions.* Services and functions will be considered "comparable" to those required by this part if the holding company:

(a) Prepares reports used by the subsidiary institution to meet the requirements of this part;

(b) Has an audit committee that meets the requirements of this part appropriate to its largest subsidiary institution; and

(c) Prepares and submits management's assessment of compliance with the Designated Laws and Regulations defined in guideline 7A and, if applicable, management's assessment of the effectiveness of internal control over financial reporting based on information concerning the relevant activities and operations of those subsidiary institutions within the scope of the Rule.

4A. *Financial Statements Prepared for Regulatory Reporting Purposes.* (a) As set forth in §363.3(c) of this part, "financial reporting," at a minimum, includes both financial statements prepared in accordance with generally accepted accounting principles for the insured depository institution or its holding company and financial statements prepared for regulatory reporting purposes. More specifically, financial statements prepared for regulatory reporting purposes include the schedules equivalent to the basic financial statements that are included in an insured depository institution's or its holding company's appropriate regulatory report (for example, Schedules RC, RL, and RI-A in the Consolidated Reports of Condition and Income (Call Report) for an insured bank; and

Schedules SC and SO, and the Summary of Changes in Equity Capital section in Schedule SI in the Thrift Financial Report (TFR) for an insured thrift institution). For recognition and measurement purposes, financial statements prepared for regulatory reporting purposes shall conform to generally accepted accounting principles and section 37 of the Federal Deposit Insurance Act.

(b) Financial statements prepared for regulatory reporting purposes do not include regulatory reports prepared by a non-bank subsidiary of a holding company or an institution. For example, if a bank holding company or an insured depository institution owns an insurance subsidiary, financial statements prepared for regulatory reporting purposes would not include any regulatory reports that the insurance subsidiary is required to submit to its appropriate insurance regulatory agency.

ANNUAL REPORTING REQUIREMENTS (§363.2)

5. *Annual Financial Statements.* Each institution (other than an insured branch of a foreign bank) should prepare comparative annual consolidated financial statements (balance sheets and statements of income, changes in equity capital, and cash flows, with accompanying footnote disclosures) in accordance with GAAP for each of its two most recent fiscal years. Statements for the earlier year may be presented on an unaudited basis if the institution was not subject to this part for that year and audited statements were not prepared.

5A. *Institutions Merged Out of Existence.* An institution that is merged out of existence after the end of its fiscal year, but before the deadline for filing its Part 363 Annual Report (120 days after the end of its fiscal year for an institution that is neither a public company nor a subsidiary of a public company that meets the criterion specified in §363.1(b)(1), and 90 days after the end of its fiscal year for an institution that is a public company or a subsidiary of a public company that meets the criterion specified in §363.1(b)(1)), is not required to file a Part 363 Annual Report for the last fiscal year of its existence.

6. *Holding Company Statements.* Subject to the criterion specified in §363.1(b)(1), subsidiary institutions may file copies of their holding company's audited financial statements filed with the SEC or prepared for their FR Y-6 Annual Report under the Bank Holding Company Act of 1956 to satisfy the audited financial statements requirement of §363.2(a).

7. *Insured Branches of Foreign Banks.* An insured branch of a foreign bank should satisfy the financial statements requirement by filing one of the following for each of its two most recent fiscal years:

(a) Audited balance sheets, disclosing information about financial instruments with off-balance-sheet risk;

(b) Schedules RAL and L of form FFIEC 002, prepared and audited on the basis of the instructions for its preparation; or

(c) With written approval of the appropriate Federal banking agency, consolidated financial statements of the parent bank.

7A. *Compliance with Designated Laws and Regulations.* The designated laws and regulations are the Federal laws and regulations concerning loans to insiders and the Federal and, if applicable, State laws and regulations concerning dividend restrictions (the Designated Laws and Regulations). Table 1 to this Appendix A lists the designated Federal laws and regulations pertaining to insider loans and dividend restrictions (but not the State laws and regulations pertaining to dividend restrictions) that are applicable to each type of institution.

8. *Management Report.* Management should perform its own investigation and review of compliance with the Designated Laws and Regulations and, if required, the effectiveness of internal control over financial reporting. Management should maintain records of its determinations and assessments until the next Federal safety and soundness examination, or such later date as specified by the FDIC or the appropriate Federal banking agency. Management should provide in its assessment of the effectiveness of internal control over financial reporting, or supplementally, sufficient information to enable the accountant to report on its assertions. The management report of an insured branch of a foreign bank should be signed by the branch's managing official if the branch does not have a chief executive officer or a chief accounting or financial officer.

8A. *Management's Reports on Internal Control over Financial Reporting under Part 363 and Section 404 of SOX.* An institution with \$1 billion or more in total assets as of the beginning of its fiscal year that is subject to both part 363 and the SEC's rules implementing section 404 of SOX (as well as a public holding company permitted under the holding company exception in §363.1(b)(2) to file an internal control report on behalf of one or more subsidiary institutions with \$1 billion or more in total assets) can choose either of the following two options for filing management's report on internal control over financial reporting.

(i) Management can prepare two separate reports on the institution's or the holding company's internal control over financial reporting to satisfy the FDIC's part 363 requirements and the SEC's section 404 requirements; or

(ii) Management can prepare a single report on internal control over financial reporting provided that it satisfies all of the

FDIC's part 363 requirements and all of the SEC's section 404 requirements.

8B. *Internal Control Reports and Part 363 Annual Reports for Acquired Businesses.* Generally, the FDIC expects management's and the related independent public accountant's report on an institution's internal control over financial reporting to include controls at an institution in its entirety, including all of its consolidated entities. However, it may not always be possible for management to conduct an assessment of the internal control over financial reporting of an acquired business in the period between the consummation date of the acquisition and the due date of management's internal control assessment.

(a) In such instances, the acquired business's internal control structure and procedures for financial reporting may be excluded from management's assessment report and the accountant's attestation report on internal control over financial reporting. However, the FDIC expects management's assessment report to identify the acquired business, state that the acquired business is excluded, and indicate the significance of this business to the institution's consolidated financial statements. Notwithstanding management's exclusion of the acquired business's internal control from its assessment, management should disclose any material change to the institution's internal control over financial reporting due to the acquisition of this business. Also, management may not omit the assessment of the acquired business's internal control from more than one annual part 363 assessment report on internal control over financial reporting. When the acquired business's internal control over financial reporting is excluded from management's assessment, the independent public accountant may likewise exclude this acquired business's internal control over financial reporting from the accountant's evaluation of internal control over financial reporting.

(b) If the acquired business is or has a consolidated subsidiary that is an insured depository institution subject to part 363 and the institution is not merged out of existence before the deadline for filing its Part 363 Annual Report (120 days after the end of its fiscal year for an institution that is neither a public company nor a subsidiary of a public company that meets the criterion specified in § 363.1(b)(1), and 90 days after the end of its fiscal year for an institution that is a public company or a subsidiary of public company that meets the criterion specified in § 363.1(b)(1)), the acquired institution must continue to comply with all of the applicable requirements of part 363, including filing its Part 363 Annual Report.

8C. *Management's Disclosure of Noncompliance with the Designated Laws and Regulations.* Management's disclosure of noncompliance,

if any, with the Designated Laws and Regulations should separately indicate the number of instances or frequency of noncompliance with the Federal laws and regulations pertaining to insider loans and the Federal (and, if applicable, State) laws and regulations pertaining to dividend restrictions. The disclosure is not required to specifically identify by name the individuals (*e.g.*, officers or directors) who were responsible for or were the subject of any such noncompliance. However, the disclosure should include appropriate qualitative and quantitative information to describe the nature, type, and severity of the noncompliance and the dollar amount of the insider loan(s) or dividend(s) involved. Similar instances of noncompliance may be aggregated as to number of instances and quantified as to the dollar amounts or the range of dollar amounts of insider loans and/or dividends for which noncompliance occurred. Management may also wish to describe any corrective actions taken in response to the instances of noncompliance as well any controls or procedures that are being developed or that have been developed and implemented to prevent or detect and correct future instances of noncompliance on a timely basis.

9. *Safeguarding of Assets.* "Safeguarding of assets," as the term relates to internal control policies and procedures regarding financial reporting and which has precedent in accounting and auditing literature, should be encompassed in the management report and the independent public accountant's attestation discussed in guideline 18. Testing the existence of and compliance with internal controls on the management of assets, including loan underwriting and documentation, represents a reasonable implementation of section 36. The FDIC expects such internal controls to be encompassed by the assertion in the management report, but the term "safeguarding of assets" need not be specifically stated. The FDIC does not require the accountant to attest to the adequacy of safeguards, but does require the accountant to determine whether safeguarding policies exist.¹⁵

10. *Standards for Internal Control.* The management of each insured depository institution with \$1 billion or more in total assets as of the beginning of its fiscal year should base its assessment of the effectiveness of the institution's internal control over financial reporting on a suitable, recognized control framework established by a body of experts

¹⁵It is management's responsibility to establish policies concerning underwriting and asset management and to make credit decisions. The auditor's role is to test compliance with management's policies relating to financial reporting.

that followed due-process procedures, including the broad distribution of the framework for public comment. In addition to being available to users of management's reports, a framework is suitable only when it:

- Is free from bias;
- Permits reasonably consistent qualitative and quantitative measurements of an institution's internal control over financial reporting;
- Is sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of an institution's internal control over financial reporting are not omitted; and
- Is relevant to an evaluation of internal control over financial reporting.

In the United States, *Internal Control—Integrated Framework*, including its addendum on safeguarding assets, which was published by the Committee of Sponsoring Organizations of the Treadway Commission, and is known as the COSO report, provides a suitable and recognized framework for purposes of management's assessment. Other suitable frameworks have been published in other countries or may be developed in the future. Such other suitable frameworks may be used by management and the institution's independent public accountant in assessments, attestations, and audits of internal control over financial reporting.

11. *Service Organizations.* Although service organizations should be considered in determining if internal control over financial reporting is effective, an institution's independent public accountant, its management, and its audit committee should exercise independent judgment concerning that determination. Onsite reviews of service organizations may not be necessary to prepare the report required by the Rule, and the FDIC does not intend that the Rule establish any such requirement.

12. [Reserved]

ROLE OF INDEPENDENT PUBLIC ACCOUNTANT (§363.3)

13. *General Qualifications.* To provide audit and attest services to insured depository institutions, an independent public accountant should be registered or licensed to practice as a public accountant, and be in good standing, under the laws of the State or other political subdivision of the United States in which the home office of the institution (or the insured branch of a foreign bank) is located. As required by section 36(g)(3)(A)(i), the accountant must agree to provide copies of any working papers, policies, and procedures relating to services performed under this part.

14. [Reserved]

15. *Peer Review Guidelines.* The following peer review guidelines are acceptable:

- (a) The external peer review should be conducted by an organization independent of the

accountant or firm being reviewed, as frequently as is consistent with professional accounting practices;

- (b) The peer review (other than a PCAOB inspection) should be generally consistent with AICPA Peer Review Standards; and

- (c) The review should include, if available, at least one audit on an insured depository institution or consolidated depository institution holding company.

16. [Reserved]

17. *Information to be Provided to the Independent Public Accountant.* Attention is directed to section 36(h) which requires institutions to provide specified information to their accountants. An institution also should provide its accountant with copies of any notice that the institution's capital category is being changed or reclassified under section 38 of the FDI Act, and any correspondence from the appropriate Federal banking agency concerning compliance with this part.

18. *Attestation Report and Management Letters.* The independent public accountant should provide the institution with any management letter and, if applicable, an internal control attestation report (as required by section 36(c)(1)) at the conclusion of the audit. The independent public accountant's attestation report on internal control over financial reporting must specifically include a statement as to regulatory reporting. If a holding company subsidiary relies on its holding company's management report to satisfy the Part 363 Annual Report requirements, the accountant may attest to and report on the management's assertions in one report, without reporting separately on each subsidiary covered by the Rule. The FDIC has determined that management letters are exempt from public disclosure.

18A. *Internal Control Attestation Standards for Independent Auditors.* (a) §363.3(b) provides that the independent public accountant's attestation and report on management's assertion concerning the effectiveness of an institution's internal control structure and procedures for financial reporting shall be made in accordance with generally accepted standards for attestation engagements or the PCAOB's auditing standards, if applicable. The standards that should be followed by the institution's independent public accountant concerning internal control over financial reporting for institutions with \$1 billion or more in total assets can be summarized as follows:

- (1) For an insured institution that is neither a public company nor a subsidiary of a public company, its independent public accountant need only follow the AICPA's attestation standards.

- (2) For an insured institution that is a public company that is required to comply with

the auditor attestation requirement of section 404 of SOX, its independent public accountant should follow the PCAOB's auditing standards.

(3) For an insured institution that is a public company but is not required to comply with the auditor attestation requirement of section 404 of SOX, its independent public accountant is not required to follow the PCAOB's auditing standards. In this case, the accountant need only follow the AICPA's attestation standards.

(4) For an insured institution that is a subsidiary of a public company that is required to comply with the auditor attestation requirement of section 404 of SOX, but is not itself a public company, the institution and its independent public accountant have flexibility in complying with the internal control requirements of part 363. If the conditions specified in §363.1(b)(2) are met, management and the independent public accountant may choose to report on internal control over financial reporting at the consolidated holding company level. In this situation, the independent public accountant's work would be performed for the public company in accordance with the PCAOB's auditing standards. Alternatively, the institution may choose to comply with the internal control reporting requirements of part 363 at the institution level and its independent public accountant could follow the AICPA's attestation standards.

(b) If an independent public accountant need only follow the AICPA's attestation standards, the accountant and the insured institution may instead agree to have the internal control attestation performed under the PCAOB's auditing standards.

19. *Reviews with Audit Committee and Management.* The independent public accountant should meet with the institution's audit committee to review the accountant's reports required by this part before they are filed. It also may be appropriate for the accountant to review its findings with the institution's board of directors and management.

20. *Notice of Termination.* The notice of termination required by §363.3(c) should state whether the independent public accountant agrees with the assertions contained in any notice filed by the institution under §363.4(d), and whether the institution's notice discloses all relevant reasons for the accountant's termination. Subject to the criterion specified in §363.1(b)(1) regarding compliance with the audited financial statements requirement at the holding company level, the independent public accountant for an insured depository institution that is a public company and files reports with its appropriate Federal banking agency, or is a subsidiary of a public company that files reports with the SEC, may submit the letter it furnished to management to be filed with the

institution's or the holding company's current report (e.g., SEC Form 8-K) concerning a change in accountant to satisfy the notice requirements of §363.3(c). Alternatively, if the independent public accountant confirms that management has filed a current report (e.g., SEC Form 8-K) concerning a change in accountant that satisfies the notice requirements of §363.4(d) and includes an independent public accountant's letter that satisfies the requirements of §363.3(c), the independent public accountant may rely on the current report (e.g., SEC Form 8-K) filed with the FDIC by management concerning a change in accountant to satisfy the notice requirements of §363.3(c).

21. *Reliance on Internal Auditors.* Nothing in this part or this Appendix is intended to preclude the ability of the independent public accountant to rely on the work of an institution's internal auditor.

FILING AND NOTICE REQUIREMENTS (§363.4)

22. [Reserved]

23. *Notification of Late Filing.* (a) An institution's submission of a written notice of late filing does not cure the requirement to timely file the Part 363 Annual Report or other reports or notices required by §363.4. An institution's failure to timely file is considered an apparent violation of part 363.

(b) If the late filing notice submitted pursuant to §363.4(e) relates only to a portion of a Part 363 Annual Report or any other report or notice, the insured depository institution should file the other components of the report or notice within the prescribed filing period together with a cover letter that indicates which components of its Part 363 Annual Report or other report or notice are omitted. An institution may combine the written late filing notice and the cover letter into a single notice that is submitted together with the other components of the report or notice that are being timely filed.

24. *Public Availability.* Each institution's Part 363 Annual Report should be available for public inspection at its main and branch offices no later than 15 days after it is filed with the FDIC. Alternatively, an institution may elect to mail one copy of its Part 363 Annual Report to any person who requests it. The Part 363 Annual Report should remain available to the public until the Part 363 Annual Report for the next year is available. An institution may use its Part 363 Annual Report under this part to meet the annual disclosure statement required by 12 CFR 350.3, if the institution satisfies all other requirements of 12 CFR Part 350.

25. [Reserved]

26. *Notices Concerning Accountants.* With respect to any selection, change, or termination of an independent public accountant, an institution's management and audit committee should be familiar with the notice requirements in §363.4(d) and guideline 20, and

management should send a copy of any notice required under § 363.4(d) to the independent public accountant when it is filed with the FDIC. An insured depository institution that is a public company and files reports required under the Federal securities laws with its appropriate Federal banking agency, or is a subsidiary of a public company that files such reports with the SEC, may use its current report (*e.g.*, SEC Form 8-K) concerning a change in accountant to satisfy the notice requirements of § 363.4(d) subject to the criterion of § 363.1(b)(1) regarding compliance with the audited financial statements requirement at the holding company level.

AUDIT COMMITTEES (§ 363.5)

27. *Composition.* The board of directors of each institution should determine whether each existing or potential audit committee member meets the requirements of section 36 and this part. To do so, the board of directors should maintain an approved set of written criteria for determining whether a director who is to serve on the audit committee is an outside director (as defined in § 363.5(a)(3)) and is independent of management. At least annually, the board of each institution should determine whether each existing or potential audit committee member is an outside director. In addition, at least annually, the board of an institution with \$1 billion or more in total assets as of the beginning of its fiscal year should determine whether all existing and potential audit committee members are “independent of management of the institution” and the board of an institution with total assets of \$500 million or more but less than \$1 billion as of the beginning of its fiscal year should determine whether the majority of all existing and potential audit committee members are “independent of management of the institution.” The minutes of the board of directors should contain the results of and the basis for its determinations with respect to each existing and potential audit committee member. Because an insured branch of a foreign bank does not have a separate board of directors, the FDIC will not apply the audit committee requirements to such branch. However, any such branch is encouraged to make a reasonable good faith effort to see that similar duties are performed by persons whose experience is generally consistent with the Rule’s requirements for an institution the size of the insured branch.

28. *“Independent of Management” Considerations.* It is not possible to anticipate, or explicitly provide for, all circumstances that might signal potential conflicts of interest in, or that might bear on, an outside director’s relationship to an insured depository institution and whether the outside director should be deemed “independent of manage-

ment.” When assessing an outside director’s relationship with an institution, the board of directors should consider the issue not merely from the standpoint of the director himself or herself, but also from the standpoint of persons or organizations with which the director has an affiliation. These relationships can include, but are not limited to, commercial, banking, consulting, charitable, and family relationships. To assist boards of directors in fulfilling their responsibility to determine whether existing and potential members of the audit committee are “independent of management,” paragraphs (a) through (d) of this guideline provide guidance for making this determination.

(a) If an outside director, either directly or indirectly, owns or controls, or has owned or controlled within the preceding fiscal year, 10 percent or more of any outstanding class of voting securities of the institution, the institution’s board of directors should determine, and document its basis and rationale for such determination, whether such ownership of voting securities would interfere with the outside director’s exercise of independent judgment in carrying out the responsibilities of an audit committee member, including the ability to evaluate objectively the propriety of management’s accounting, internal control, and reporting policies and practices. Notwithstanding the criteria set forth in paragraphs (b), (c), and (d) of this guideline, if the board of directors determines that such ownership of voting securities would interfere with the outside director’s exercise of independent judgment, the outside director will not be considered “independent of management.”

(b) The following list sets forth additional criteria that, at a minimum, a board of directors should consider when determining whether an outside director is “independent of management.” The board of directors may conclude that additional criteria are also relevant to this determination in light of the particular circumstances of its institution. Accordingly, an outside director will not be considered “independent of management” if:

- (1) The director serves, or has served within the last three years, as a consultant, advisor, promoter, underwriter, legal counsel, or trustee of or to the institution or its affiliates.

- (2) The director has been, within the last three years, an employee of the institution or any of its affiliates or an immediate family member is, or has been within the last three years, an executive officer of the institution or any of its affiliates.

- (3) The director has participated in the preparation of the financial statements of the institution or any of its affiliates at any time during the last three years.

- (4) The director has received, or has an immediate family member who has received, during any twelve-month period within the

last three years, more than \$100,000 in direct and indirect compensation from the institution, its subsidiaries, and its affiliates for consulting, advisory, or other services other than director and committee fees and pension or other forms of deferred compensation for prior service (provided such compensation is not contingent in any way on continued service). Direct compensation also would not include compensation received by the director for former service as an interim chairman or interim chief executive officer.

(5) The director or an immediate family member is a current partner of a firm that performs internal or external auditing services for the institution or any of its affiliates; the director is a current employee of such a firm; the director has an immediate family member who is a current employee of such a firm and who participates in the firm's audit, assurance, or tax compliance practice; or the director or an immediate family member was within the last three years (but no longer is) a partner or employee of such a firm and personally worked on the audit of the insured depository institution or any of its affiliates within that time.

(6) The director or an immediate family member is, or has been within the last three years, employed as an executive officer of another entity where any of the present executive officers of the institution or any of its affiliates at the same time serves or served on that entity's compensation committee.

(7) The director is a current employee, or an immediate family member is a current executive officer, of an entity that has made payments to, or received payments from, the institution or any of its affiliates for property or services in an amount which, in any of the last three fiscal years, exceeds the greater of \$200 thousand, or 5 percent of such entity's consolidated gross revenues. This would include payments made by the institution or any of its affiliates to not-for-profit entities where the director is an executive officer or where an immediate family member of the director is an executive officer.

(8) For purposes of paragraph (b) of this guideline:

(i) An "immediate family member" includes a person's spouse, parents, children, siblings, mothers- and fathers-in-law, sons- and daughters-in-law, brothers- and sisters-in-law, and anyone (other than domestic employees) who shares such person's home.

(ii) The term affiliate of, or a person affiliated with, a specified person, means a person or entity that directly, or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with, the person specified.

(iii) The term indirect compensation for consulting, advisory, or other services includes the acceptance of a fee for such serv-

ices by a director's immediate family member or by an organization in which the director is a partner or principal that provides accounting, consulting, legal, investment banking, or financial advisory services to the institution, any of its subsidiaries, or any of its affiliates.

(iv) The terms direct and indirect compensation and payments do not include payments such as dividends arising solely from investments in the institution's equity securities, provided the same per share amounts are paid to all shareholders of that class; interest income from investments in the institution's deposit accounts and debt securities; loans from the institution that conform to all regulatory requirements applicable to such loans except that interest payments or other fees paid in association with such loans would be considered payments; and payments under non-discretionary charitable contribution matching programs.

(c) An insured depository institution that is a public company and a listed issuer (as defined in Rule 10A-3 of the Securities Exchange Act of 1934 (Exchange Act)), or is a subsidiary of a public company that meets the criterion specified in § 363.1(b)(1) and is a listed issuer, may choose to use the definition of audit committee member independence set forth in the listing standards applicable to the public institution or its public company parent for purposes of determining whether an outside director is "independent of management."

(d) All other insured depository institutions may choose to use the definition of audit committee member independence set forth in the listing standards of a national securities exchange that is registered with the SEC pursuant to section 6 of the Exchange Act or a national securities association that is registered with the SEC pursuant to section 15A(a) of the Exchange Act for purposes of determining whether an outside director is "independent of management."

29. [Reserved]

30. *Holding Company Audit Committees.* (a) When an insured depository institution satisfies the requirements for the holding company exception specified in §§ 363.1(b)(1) and (2), the audit committee requirement of this part may be satisfied by the audit committee of the top-tier or any mid-tier holding company. Members of the audit committee of the holding company should meet all the membership requirements applicable to the largest subsidiary depository institution subject to part 363 and should perform all the duties of the audit committee of a subsidiary institution subject to part 363, even if the holding company directors are not directors of the institution.

(b) When an insured depository institution subsidiary with total assets of \$1 billion or more as of the beginning of its fiscal year

does not meet the requirements for the holding company exception specified in §§363.1(b)(1) and (2) or maintains its own separate audit committee to satisfy the requirements of this part, the members of the audit committee of the top-tier or any mid-tier holding company may serve on the audit committee of the subsidiary institution if they are otherwise independent of management of the subsidiary institution, and, if applicable, meet any other requirements for a large subsidiary institution covered by this part.

(c) When an insured depository institution with total assets of \$500 million or more but less than \$1 billion as of the beginning of its fiscal year does not meet the requirements for the holding company exception specified in §§363.1(b)(1) and (2) or maintains its own separate audit committee to satisfy the requirements of this part, the members of the audit committee of the top-tier or any mid-tier holding company may serve on the audit committee of the subsidiary institution provided a majority of the institution's audit committee members are independent of management of the subsidiary institution.

(d) Officers and employees of a top-tier or any mid-tier holding company may not serve on the audit committee of a subsidiary institution subject to part 363.

31. *Duties.* The audit committee should perform all duties determined by the institution's board of directors and it should maintain minutes and other relevant records of its meetings and decisions. The duties of the audit committee should be appropriate to the size of the institution and the complexity of its operations, and, at a minimum, should include the appointment, compensation, and oversight of the independent public accountant; reviewing with management and the independent public accountant the basis for their respective reports issued under §§363.2(a) and (b) and §§363.3(a) and (b); reviewing and satisfying itself as to the independent public accountant's compliance with the required qualifications for independent public accountants set forth in §§363.3(f) and (g) and guidelines 13 through 16; ensuring that audit engagement letters comply with the provisions of §363.5(c) before engaging an independent public accountant; being familiar with the notice requirements in §363.4(d) and guideline 20 regarding the selection, change, or termination of an independent public accountant; and ensuring that management sends a copy of any notice required under §363.4(d) to the independent public accountant when it is filed with the FDIC. Appropriate additional duties could include:

(a) Reviewing with management and the independent public accountant the scope of services required by the audit, significant accounting policies, and audit conclusions regarding significant accounting estimates;

(b) Reviewing with management and the accountant their assessments of the effectiveness of internal control over financial reporting, and the resolution of identified material weaknesses and significant deficiencies in internal control over financial reporting, including the prevention or detection of management override or compromise of the internal control system;

(c) Reviewing with management the institution's compliance with the Designated Laws and Regulations identified in guideline 7A;

(d) Discussing with management and the independent public accountant any significant disagreements between management and the independent public accountant; and

(e) Overseeing the internal audit function.

32. *Banking or Related Financial Management Expertise.* At least two members of the audit committee of a large institution shall have "banking or related financial management expertise" as required by section 36(g)(1)(C)(i). This determination is to be made by the board of directors of the insured depository institution. A person will be considered to have such required expertise if the person has significant executive, professional, educational, or regulatory experience in financial, auditing, accounting, or banking matters as determined by the board of directors. Significant experience as an officer or member of the board of directors or audit committee of a financial services company would satisfy these criteria. A person who has the attributes of an "audit committee financial expert" as set forth in the SEC's rules would also satisfy these criteria.

33. *Large Customers.* Any individual or entity (including a controlling person of any such entity) which, in the determination of the board of directors, has such significant direct or indirect credit or other relationships with the institution, the termination of which likely would materially and adversely affect the institution's financial condition or results of operations, should be considered a "large customer" for purposes of §363.5(b).

34. *Access to Counsel.* The audit committee should be able to retain counsel at its discretion without prior permission of the institution's board of directors or its management. Section 36 does not preclude advice from the institution's internal counsel or regular outside counsel. It also does not require retaining or consulting counsel, but if the committee elects to do either, it also may elect to consider issues affecting the counsel's independence. Such issues would include whether to retain or consult only counsel not concurrently representing the institution or any affiliate, and whether to place limitations on any counsel representing the institution concerning matters in which

Federal Deposit Insurance Corporation

Pt. 363, App. A

such counsel previously participated personally and substantially as outside counsel to the committee.

35. Transition Period for Forming and Restructuring Audit Committees.

(a) When an insured depository institution's total assets as of the beginning of its fiscal year are \$500 million or more for the first time and it thereby becomes subject to part 363, no regulatory action will be taken if the institution (1) develops and approves a set of written criteria for determining whether a director who is to serve on the audit committee is an outside director and is independent of management and (2) forms or restructures its audit committee to comply with §363.5(a)(2) by the end of that fiscal year.

(b) When an insured depository institution's total assets as of the beginning of its fiscal year are \$1 billion or more for the first time, no regulatory action will be taken if the institution forms or restructures its audit committee to comply with §363.5(a)(1) by the end of that fiscal year, provided that the composition of its audit committee meets the requirements specified in §363.5(a)(2) at the beginning of that fiscal year, if such requirements were applicable.

(c) When an insured depository institution's total assets as of the beginning of its

fiscal year are \$3 billion or more for the first time, no regulatory action will be taken if the institution forms or restructures its audit committee to comply with §363.5(b) by the end of that fiscal year, provided that the composition of its audit committee meets the requirements specified in §363.5(a)(1) at the beginning of that fiscal year, if such requirements were applicable.

OTHER

36. Modifications of Guidelines. The FDIC's Board of Directors has delegated to the Director of the FDIC's Division of Supervision and Consumer Protection authority to make and publish in the FEDERAL REGISTER minor technical amendments to the Guidelines in this Appendix and the guidance and illustrative reports in Appendix B, in consultation with the other appropriate Federal banking agencies, to reflect the practical experience gained from implementation of this part. It is not anticipated any such modification would be effective until affected institutions have been given reasonable advance notice of the modification. Any material modification or amendment will be subject to review and approval of the FDIC Board of Directors.

TABLE 1 TO APPENDIX A—DESIGNATED FEDERAL LAWS AND REGULATIONS APPLICABLE TO:

		National banks	State member banks	State non-member banks	Savings associations
Insider Loans—Parts and/or Sections of Title 12 of the United States Code					
375a	Loans to Executive Officers of Banks	√	√	(A)	(A)
375b	Extensions of Credit to Executive Officers, Directors, and Principal Shareholders of Banks.	√	√	(A)	(A)
1468(b)	Extensions of Credit to Executive Officers, Directors, and Principal Shareholders.	√
1828(j)(2)	Extensions of Credit to Officers, Directors, and Principal Shareholders.	√
1828(j)(3)(B)	Extensions of Credit to Officers, Directors, and Principal Shareholders.	(B)	(C)
Parts and/or Sections of Title 12 of the Code of Federal Regulations					
31	Extensions of Credit to Insiders	√
32	Lending Limits	√
215	Loans to Executive Officers, Directors, and Principal Shareholders of Member Banks.	√	√	(D)	(E)
337.3	Limits on Extensions of Credit to Executive Officers, Directors, and Principal Shareholders of Insured Nonmember Banks.	√
563.43	Loans by Savings Associations to Their Executive Officers, Directors, and Principal Shareholders.	√
Dividend Restrictions—Parts and/or Sections of Title 12 of the United States Code					
56	Prohibition on Withdrawal of Capital and Unearned Dividends.	√	√
60	Dividends and Surplus Fund	√	√

TABLE 1 TO APPENDIX A—DESIGNATED FEDERAL LAWS AND REGULATIONS APPLICABLE TO:—
Continued

		National banks	State member banks	State non-member banks	Savings associations
1467a(f)	Declaration of Dividend	√
1831o(d)(1)	Prompt Corrective Action—Capital Distributions Restricted.	√	√	√	√
Parts and/or Sections of Title 12 of the Code of Federal Regulations					
5 Subpart E	Payment of Dividends	√
6.6	Prompt Corrective Action—Restrictions on Undercapitalized Institutions.	√
208.5	Dividends and Other Distributions	√
208.45	Prompt Corrective Action—Restrictions on Undercapitalized Institutions.	√
325.105	Prompt Corrective Action—Restrictions on Undercapitalized Institutions.	√
563 Subpart E	Capital Distributions	√
565.6	Prompt Corrective Action—Restrictions on Undercapitalized Institutions.	√

- A. Subsections (g) and (h) of section 22 of the Federal Reserve Act [12 U.S.C. 375a, 375b]
- B. Applies only to insured Federal branches of foreign banks.
- C. Applies only to insured State branches of foreign banks.
- D. See 12 CFR 337.3.
- E. See 12 CFR 563.43.

APPENDIX B TO PART 363—ILLUSTRATIVE MANAGEMENT REPORTS

TABLE OF CONTENTS

1. General
2. Reporting Scenarios for Institutions that are Holding Company Subsidiaries
3. Illustrative Statements of Management’s Responsibilities
4. Illustrative Reports on Management’s Assessment of Compliance with Designated Laws and Regulations
5. Illustrative Reports on Management’s Assessment of Internal Control Over Financial Reporting
6. Illustrative Management Report—Combined Statement of Management’s Responsibilities, Report on Management’s Assessment of Compliance With Designated Laws and Regulations, and Report on Management’s Assessment of Internal Control Over Financial Reporting
7. Illustrative Cover Letter—Compliance by Holding Company Subsidiaries

1. *General.* The reporting scenarios, illustrative management reports, and the cover letter (when complying at the holding company level) in Appendix B to part 363 are intended to assist managements of insured depository institutions in complying with the annual reporting requirements of §363.2 and guideline 3, *Compliance by Holding Company Subsidiaries*, of Appendix A to part 363. However, use of the illustrative management re-

ports and cover letter is not required. The managements of insured depository institutions are encouraged to tailor the wording of their management reports and cover letters to fit their particular circumstances, especially when reporting on material weaknesses in internal control over financial reporting or noncompliance with designated laws and regulations. Terms that are not explained in Appendix B have the meanings given them in part 363, the FDI Act, or professional accounting and auditing literature. Instructions to the preparer of the management reports are shown in brackets within the illustrative reports.

2. *Reporting Scenarios for Institutions that are Holding Company Subsidiaries.* (a) Subject to the criteria specified in §363.1(b), an insured depository institution that is a subsidiary of a holding company has flexibility in satisfying the reporting requirements of part 363. When reporting at the holding company level, the management report, or the individual components thereof, should identify those subsidiary institutions that are subject to part 363 and the extent to which they are included in the scope of the management report or a component of the report. The following reporting scenarios reflect how an insured depository institution that meets the criteria set forth in §363.1(b) could satisfy the annual reporting requirements of §363.2. Other reporting scenarios are possible.

(i) An institution that is a subsidiary of a holding company may satisfy the requirements for audited financial statements; management's statement of responsibilities; management's assessment of the institution's compliance with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions; management's assessment of the effectiveness of internal control over financial reporting, if applicable; and the independent public accountant's attestation on management's assertion as to the effectiveness of internal control over financial reporting, if applicable, at the insured depository institution level.

(ii) An institution that is a subsidiary of a holding company may satisfy the requirements for audited financial statements; management's statement of responsibilities; management's assessment of the institution's compliance with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions; management's assessment of the effectiveness of internal control over financial reporting, if applicable; and the independent public accountant's attestation on management's assertion as to the effectiveness of internal control over financial reporting, if applicable, at the holding company level.

(iii) An institution that is a subsidiary of a holding company may satisfy the requirement for audited financial statements at the holding company level and may satisfy the requirements for management's statement of responsibilities; management's assessment of the institution's compliance with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions; management's assessment of the effectiveness of internal control over financial reporting, if applicable; and the independent public accountant's attestation on management's assertion as to the effectiveness of internal control over financial reporting, if applicable, at the insured depository institution level.

(iv) An institution that is a subsidiary of a holding company may satisfy the requirements for audited financial statements; management's statement of responsibilities; and management's assessment of the institution's compliance with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions at the insured depository institution level and may satisfy the requirements for the assessment by management of the effectiveness of internal control over financial reporting, if applicable; and the independent public accountant's attestation on management's assertion as to the effectiveness of in-

ternal control over financial reporting, if applicable, at the holding company level.

(b) For an institution with total assets of \$1 billion or more as of the beginning of its fiscal year, the assessment by management of the effectiveness of internal control over financial reporting and the independent public accountant's attestation on management's assertion as to the effectiveness of internal control over financial reporting, if applicable, must both be performed at the same level, *i.e.*, either at the insured depository institution level or at the holding company level.

(c) Financial statements prepared for regulatory reporting purposes encompass the schedules equivalent to the basic financial statements in an institution's appropriate regulatory report, *e.g.*, the bank Consolidated Reports of Condition and Income (Call Report) and the Thrift Financial Report (TFR). Guideline 4A in Appendix A to part 363 identifies the schedules equivalent to the basic financial statements in the Call Report and TFR. When internal control assessments and attestations are performed at the holding company level, the FDIC believes that holding companies have flexibility in interpreting "financial reporting" as it relates to "regulatory reporting" and has not objected to several reporting approaches employed by holding companies to cover "regulatory reporting." Certain holding companies have had management's assessment and the accountant's attestation cover the schedules equivalent to the basic financial statements that are included in the appropriate regulatory report, *e.g.*, Call Report and the TFR, of each subsidiary institution subject to part 363. Other holding companies have had management's assessment and the accountant's attestation cover the schedules equivalent to the basic financial statements that are included in the holding company's year-end regulatory report (FR Y-9C report) to the Federal Reserve Board.

3. *Illustrative Statements of Management's Responsibilities.* The following illustrative statements of management's responsibilities satisfy the requirements of §363.2(b)(1).

(a) Statement Made at Insured Depository Institution Level

STATEMENT OF MANAGEMENT'S
RESPONSIBILITIES

The management of ABC Depository Institution (the "Institution") is responsible for preparing the Institution's annual financial statements in accordance with generally accepted accounting principles; for establishing and maintaining an adequate internal control structure and procedures for financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report]; and

Pt. 363, App. B

12 CFR Ch. III (1–13 Edition)

for complying with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions.

ABC Depository Institution

John Doe, Chief Executive Officer

Date: _____

Jane Doe, Chief Financial Officer

Date: _____

(b) Statement Made at Holding Company Level

STATEMENT OF MANAGEMENT'S RESPONSIBILITIES

The management of BCD Holding Company (the "Company") is responsible for preparing the Company's annual financial statements in accordance with generally accepted accounting principles; for establishing and maintaining an adequate internal control structure and procedures for financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report]; and for complying with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions. The following subsidiary institutions of the Company that are subject to Part 363 are included in this statement of management's responsibilities: [Identify the subsidiary institutions.]

BCD Holding Company

John Doe, Chief Executive Officer

Date: _____

Jane Doe, Chief Financial Officer

Date: _____

4. *Illustrative Reports on Management's Assessment of Compliance with Designated Laws and Regulations.* The following illustrative reports on management's assessment of compliance with Designated Laws and Regulations satisfy the requirements of §363.2(b)(2).

(a) Statement Made at Insured Depository Institution Level—Compliance With Designated Laws and Regulations Pertaining to Insider Loans and Dividend Restrictions

MANAGEMENT'S ASSESSMENT OF COMPLIANCE WITH DESIGNATED LAWS AND REGULATIONS

The management of ABC Depository Institution (the "Institution") has assessed the Institution's compliance with the Federal

laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions during the fiscal year that ended on December 31, 20XX. Based upon its assessment, management has concluded that the Institution complied with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions during the fiscal year that ended on December 31, 20XX.

ABC Depository Institution

John Doe, Chief Executive Officer

Date: _____

Jane Doe, Chief Financial Officer

Date: _____

(b) Statement Made at Insured Depository Institution Level—Noncompliance With Designated Laws and Regulations Pertaining to Both Insider Loans and Dividend Restrictions

MANAGEMENT'S ASSESSMENT OF COMPLIANCE WITH DESIGNATED LAWS AND REGULATIONS

The management of ABC Depository Institution (the "Institution") has assessed the Institution's compliance with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions during the fiscal year that ended on December 31, 20XX. Based upon its assessment, management has determined that, because of the instance(s) of non-compliance noted below, the Institution did not comply with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions during the fiscal year that ended on December 31, 20XX.

[Identify and describe the instance or instances of noncompliance with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions, including appropriate qualitative and quantitative information to describe the nature, type, and severity of the noncompliance and the dollar amounts of the insider loan(s) and dividend(s) involved.]

ABC Depository Institution

John Doe, Chief Executive Officer

Date: _____

Jane Doe, Chief Financial Officer

Date: _____

Federal Deposit Insurance Corporation

Pt. 363, App. B

(c) Statement Made at Insured Depository Institution Level—Compliance With Designated Laws and Regulations Pertaining to Insider Loans and Noncompliance With Designated Laws and Regulations Pertaining to Dividend Restrictions

MANAGEMENT’S ASSESSMENT OF COMPLIANCE WITH DESIGNATED LAWS AND REGULATIONS

The management of ABC Depository Institution (the “Institution”) has assessed the Institution’s compliance with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions during the fiscal year that ended on December 31, 20XX. Based upon its assessment, management has concluded that the Institution complied with the Federal laws and regulations pertaining to insider loans during the fiscal year that ended on December 31, 20XX. Also, based upon its assessment, management has determined that, because of the instance(s) of noncompliance noted below, the Institution did not comply with the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions during the fiscal year that ended on December 31, 20XX.

[Identify and describe the instance or instances of noncompliance with the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions, including appropriate qualitative and quantitative information to describe the nature, type, and severity of the noncompliance and the dollar amount(s) of the dividend(s) involved.]

ABC Depository Institution

John Doe, Chief Executive Officer
Date: _____

Jane Doe, Chief Financial Officer
Date: _____

(d) Statement Made at Insured Depository Institution Level—Noncompliance With Designated Laws and Regulations Pertaining to Insider Loans and Compliance With Designated Laws and Regulations Pertaining to Dividend Restrictions

MANAGEMENT’S ASSESSMENT OF COMPLIANCE WITH DESIGNATED LAWS AND REGULATIONS

The management of ABC Depository Institution (the “Institution”) has assessed the Institution’s compliance with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions during the fiscal year that ended on December 31, 20XX. Based upon its assessment, management has determined that, because of the instance(s) of non-compliance noted below, the Institution did

not comply with the Federal laws and regulations pertaining to insider loans during the fiscal year that ended on December 31, 20XX. Also, based upon its assessment, management has concluded that the Institution complied with the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions during the fiscal year that ended on December 31, 20XX.

[Identify and describe the instance or instances of noncompliance with the Federal laws and regulations pertaining to insider loans, including appropriate qualitative and quantitative information to describe the nature, type, and severity of the noncompliance and the dollar amount(s) of the insider loan(s) involved.]

ABC Depository Institution

John Doe, Chief Executive Officer
Date: _____

Jane Doe, Chief Financial Officer
Date: _____

(e) Statement Made at Holding Company Level—Compliance With Designated Laws and Regulations Pertaining to Insider Loans and Dividend Restrictions

MANAGEMENT’S ASSESSMENT OF COMPLIANCE WITH DESIGNATED LAWS AND REGULATIONS

The management of BCD Holding Company (the “Company”) has assessed the Company’s compliance with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions during the fiscal year that ended on December 31, 20XX. Based upon its assessment, management has concluded that the Company complied with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions during the fiscal year that ended on December 31, 20XX. The following subsidiary institutions of the Company that are subject to Part 363 are included in this assessment of compliance with these designated laws and regulations: [Identify the subsidiary institutions.]

BCD Holding Company

John Doe, Chief Executive Officer
Date: _____

Jane Doe, Chief Financial Officer
Date: _____

(f) Statement Made at Holding Company Level—Noncompliance With Designated Laws and Regulations Pertaining to Both Insider Loans and Dividend Restrictions

MANAGEMENT’S ASSESSMENT OF COMPLIANCE WITH DESIGNATED LAWS AND REGULATIONS

The management of BCD Holding Company (the “Company”) has assessed the Company’s compliance with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions during the fiscal year that ended on December 31, 20XX. The following subsidiary institutions of the Company that are subject to Part 363 are included in this assessment of compliance with these designated laws and regulations: [Identify the subsidiary institutions.]

Based upon its assessment, management has determined that, because of the instance(s) of noncompliance noted below, the Company did not comply with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions during the fiscal year that ended on December 31, 20XX.

[Identify and describe the instance or instances of noncompliance with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions, including appropriate qualitative and quantitative information to identify the subsidiary institutions of the Company that are subject to Part 363 that had instances of noncompliance and describe the nature, type, and severity of the non-compliance and the dollar amount(s) of the insider loan(s) and dividend(s) involved.]

BCD Holding Company

John Doe, Chief Executive Officer
Date: _____

Jane Doe, Chief Financial Officer
Date: _____

(g) Statement Made at Holding Company Level—Compliance With Designated Laws and Regulations Pertaining to Insider Loans and Noncompliance With Designated Laws and Regulations Pertaining to Dividend Restrictions

MANAGEMENT’S ASSESSMENT OF COMPLIANCE WITH DESIGNATED LAWS AND REGULATIONS

The management of BCD Holding Company (the “Company”) has assessed the Company’s compliance with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restric-

tions during the fiscal year that ended on December 31, 20XX. The following subsidiary institutions of the Company that are subject to Part 363 are included in this assessment of compliance with these designated laws and regulations: [Identify the subsidiary institutions.]

Based upon its assessment, management has concluded that the Company complied with the Federal laws and regulations pertaining to insider loans during the fiscal year that ended on December 31, 20XX. Also, based upon its assessment, management has determined that, because of the instance(s) of noncompliance noted below, the Company did not comply with the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions during the fiscal year that ended on December 31, 20XX.

[Identify and describe the instance or instances of noncompliance with the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions, including appropriate qualitative and quantitative information to identify the subsidiary institutions of the Company that are subject to Part 363 that had instances of noncompliance and describe the nature, type, and severity of the noncompliance and the dollar amount(s) of the dividend(s) involved.]

BCD Holding Company

John Doe, Chief Executive Officer
Date: _____

Jane Doe, Chief Financial Officer
Date: _____

(h) Statement Made at Holding Company Level—Noncompliance With Designated Laws and Regulations Pertaining to Insider Loans and Compliance With Designated Laws and Regulations Pertaining to Dividend Restrictions

MANAGEMENT’S ASSESSMENT OF COMPLIANCE WITH DESIGNATED LAWS AND REGULATIONS

The management of BCD Holding Company (the “Company”) has assessed the Company’s compliance with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions during the fiscal year that ended on December 31, 20XX. The following subsidiary institutions of the Company that are subject to Part 363 are included in this assessment of compliance with these designated laws and regulations: [Identify the subsidiary institutions.]

Based upon its assessment, management has determined that, because of the instance(s) of noncompliance noted below, the Company did not comply with the Federal laws and regulations pertaining to insider

Federal Deposit Insurance Corporation

Pt. 363, App. B

loans during the fiscal year that ended on December 31, 20XX. Also, based upon its assessment, management has concluded that the Company complied with the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions during the fiscal year that ended on December 31, 20XX.

[Identify and describe the instance or instances of noncompliance with the Federal laws and regulations pertaining to insider loans, including appropriate qualitative and quantitative information to identify the subsidiary institutions of the Company that are subject to Part 363 that had instances of non-compliance and describe the nature, type, and severity of the noncompliance and the dollar amount(s) of the insider loan(s) involved.]

BCD Holding Company

John Doe, Chief Executive Officer

Date: _____

Jane Doe, Chief Financial Officer

Date: _____

5. Illustrative Reports on Management's Assessment of Internal Control Over Financial Reporting. The following illustrative reports on management's assessment of internal control over financial reporting satisfy the requirements of §363.2(b)(3).

(a) Statement Made at Insured Depository Institution Level—No Material Weaknesses

MANAGEMENT'S ASSESSMENT OF INTERNAL CONTROL OVER FINANCIAL REPORTING

ABC Depository Institution's (the "Institution") internal control over financial reporting is a process effected by those charged with governance, management, and other personnel, designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of reliable financial statements in accordance with accounting principles generally accepted in the United States of America and financial statements for regulatory reporting purposes, i.e., [specify the regulatory reports]. The Institution's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the Institution; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with accounting principles generally accepted in the United States of America and financial statements for regulatory reporting purposes, and that receipts and expenditures of the Institution are being made only in accordance with authorizations

of management and directors of the Institution; and (3) provide reasonable assurance regarding prevention, or timely detection and correction of unauthorized acquisition, use, or disposition of the Institution's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies and procedures may deteriorate.

Management is responsible for establishing and maintaining effective internal control over financial reporting including controls over the preparation of regulatory financial statements. Management assessed the effectiveness of the Institution's internal control over financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report], as of December 31, 20XX, based on the framework set forth by the Committee of Sponsoring Organizations of the Treadway Commission in Internal Control—Integrated Framework. Based upon its assessment, management has concluded that, as of December 31, 20XX, the Institution's internal control over financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report], is effective based on the criteria established in Internal Control—Integrated Framework.

Management's assessment of the effectiveness of internal control over financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report], as of December 31, 20XX, has been audited by [name of auditing firm], an independent public accounting firm, as stated in their report dated March XX, 20XY.

ABC Depository Institution

John Doe, Chief Executive Officer

Date: _____

Jane Doe, Chief Financial Officer

Date: _____

(b) Statement Made at Insured Depository Institution Level—One or More Material Weaknesses

MANAGEMENT’S ASSESSMENT OF INTERNAL CONTROL OVER FINANCIAL REPORTING

ABC Depository Institution’s (the “Institution”) internal control over financial reporting is a process effected by those charged with governance, management, and other personnel, designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of reliable financial statements in accordance with accounting principles generally accepted in the United States of America and financial statements for regulatory reporting purposes, i.e., [specify the regulatory reports]. The Institution’s internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the Institution; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with accounting principles generally accepted in the United States of America and financial statements for regulatory reporting purposes, and that receipts and expenditures of the Institution are being made only in accordance with authorizations of management and directors of the Institution; and (3) provide reasonable assurance regarding prevention, or timely detection and correction of unauthorized acquisition, use, or disposition of the Institution’s assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies and procedures may deteriorate.

Management is responsible for establishing and maintaining effective internal control over financial reporting including controls over the preparation of regulatory financial statements. Management assessed the effectiveness of the Institution’s internal control over financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report], as of December 31, 20XX, based on the framework set forth by the Committee of Sponsoring Organizations of the Treadway Commission in *Internal Control—Integrated Framework*. Because of the material weakness (or weaknesses) noted below, management determined that the Institution’s internal con-

trol over financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report], was not effective as of December 31, 20XX.

[Identify and describe the material weakness or weaknesses.]

Management’s assessment of the effectiveness of internal control over financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report], as of December 31, 20XX, has been audited by [name of auditing firm], an independent public accounting firm, as stated in their report dated March XX, 20XY.

ABC Depository Institution

John Doe, Chief Executive Officer

Date: _____

Jane Doe, Chief Financial Officer

Date: _____

(c) Statement Made at Holding Company Level—No Material Weaknesses

MANAGEMENT’S ASSESSMENT OF INTERNAL CONTROL OVER FINANCIAL REPORTING

BCD Holding Company’s (the “Company”) internal control over financial reporting is a process designed and effected by those charged with governance, management, and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of reliable financial statements in accordance with accounting principles generally accepted in the United States of America and financial statements for regulatory reporting purposes, i.e., [specify the regulatory reports]. The Company’s internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the Company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with accounting principles generally accepted in the United States of America and financial statements for regulatory reporting purposes, and that receipts and expenditures of the Company are being made only in accordance with authorizations of management and directors of the Company; and (3) provide reasonable assurance regarding prevention, or timely detection and correction of unauthorized acquisition, use, or disposition of the Company’s assets

that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies and procedures may deteriorate.

Management is responsible for establishing and maintaining effective internal control over financial reporting including controls over the preparation of regulatory financial statements. Management assessed the effectiveness of the Company's internal control over financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report], as of December 31, 20XX, based on the framework set forth by the Committee of Sponsoring Organizations of the Treadway Commission in *Internal Control—Integrated Framework*. Based on that assessment, management concluded that, as of December 31, 20XX, the Company's internal control over financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report], is effective based on the criteria established in *Internal Control—Integrated Framework*. The following subsidiary institutions of the Company that are subject to Part 363 are included in this assessment of the effectiveness of internal control over financial reporting: [Identify the subsidiary institutions.]

Management's assessment of the effectiveness of internal control over financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report], as of December 31, 20XX, has been audited by [name of auditing firm], an independent public accounting firm, as stated in their report dated March XX, 20XY.

BCD Holding Company

John Doe, Chief Executive Officer
Date: _____

Jane Doe, Chief Financial Officer
Date: _____

(d) Statement Made at Holding Company Level—One or More Material Weaknesses

MANAGEMENT'S ASSESSMENT OF INTERNAL CONTROL OVER FINANCIAL REPORTING

BCD Holding Company's (the "Company") internal control over financial reporting is a

process effected by those charged with governance, management, and other personnel, designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of reliable financial statements in accordance with accounting principles generally accepted in the United States of America and financial statements for regulatory reporting purposes, *i.e.*, [specify the regulatory reports]. The Company's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the Company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with accounting principles generally accepted in the United States of America and financial statements for regulatory reporting purposes, and that receipts and expenditures of the Company are being made only in accordance with authorizations of management and directors of the Company; and (3) provide reasonable assurance regarding prevention, or timely detection and correction of unauthorized acquisition, use, or disposition of the Company's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies and procedures may deteriorate.

Management is responsible for establishing and maintaining effective internal control over financial reporting including controls over the preparation of regulatory financial statements. Management assessed the effectiveness of the Company's internal control over financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report], as of December 31, 20XX, based on the framework set forth by the Committee of Sponsoring Organizations of the Treadway Commission in *Internal Control—Integrated Framework*. Because of the material weakness (or weaknesses) noted below, management determined that the Company's internal control over financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report], was not effective as of December 31, 20XX. The following subsidiary institutions of the Company that are subject to Part 363

are included in this assessment of the effectiveness of internal control over financial reporting: [Identify the subsidiary institutions.]

[Identify and describe the material weakness or weaknesses.]

Management’s assessment of the effectiveness of internal control over financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report], as of December 31, 20XX, has been audited by [name of auditing firm], an independent public accounting firm, as stated in their report dated March XX, 20XY.

BCD Holding Company

John Doe, Chief Executive Officer

Date: _____

Jane Doe, Chief Financial Officer

Date: _____

6. *Illustrative Management Report—Combined Statement of Management’s Responsibilities, Report on Management’s Assessment of Compliance With Designated Laws and Regulations, and Report on Management’s Assessment of Internal Control Over Financial Reporting*, if applicable. The following illustrative management reports satisfy the requirements of §§363.2(b)(1), (2), and (3).

(a) Management Report Made at Insured Depository Institution Level—Compliance With Designated Laws and Regulations Pertaining to Insider Loans and Dividend Restrictions and No Material Weaknesses in Internal Control Over Financial Reporting

MANAGEMENT REPORT

Statement of Management’s Responsibilities

The management of ABC Depository Institution (the “Institution”) is responsible for preparing the Institution’s annual financial statements in accordance with generally accepted accounting principles; for establishing and maintaining an adequate internal control structure and procedures for financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report]; and for complying with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions.

Management’s Assessment of Compliance With Designated Laws and Regulations

The management of the Institution has assessed the Institution’s compliance with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions during the fiscal year that ended on December 31, 20XX. Based upon its assessment, management has concluded that the Institution complied with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions during the fiscal year that ended on December 31, 20XX.

Management’s Assessment of Internal Control Over Financial Reporting

The Institution’s internal control over financial reporting is a process effected by those charged with governance, management, and other personnel, designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of reliable financial statements in accordance with accounting principles generally accepted in the United States of America and financial statements for regulatory reporting purposes, *i.e.*, [specify the regulatory reports]. The Institution’s internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the Institution; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with accounting principles generally accepted in the United States of America and financial statements for regulatory reporting purposes, and that receipts and expenditures of the Institution are being made only in accordance with authorizations of management and directors of the Institution; and (3) provide reasonable assurance regarding prevention, or timely detection and correction of unauthorized acquisition, use, or disposition of the Institution’s assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies and procedures may deteriorate.

Management assessed the effectiveness of the Institution’s internal control over financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions

Federal Deposit Insurance Corporation

Pt. 363, App. B

for the [specify the regulatory report], as of December 31, 20XX, based on the framework set forth by the Committee of Sponsoring Organizations of the Treadway Commission in *Internal Control—Integrated Framework*.

Based upon its assessment, management has concluded that, as of December 31, 20XX, the Institution's internal control over financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report], is effective based on the criteria established in *Internal Control—Integrated Framework*.

Management's assessment of the effectiveness of internal control over financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report], as of December 31, 20XX, has been audited by [name of auditing firm], an independent public accounting firm, as stated in their report dated March XX, 20XY.

ABC Depository Institution

John Doe, Chief Executive Officer
Date: _____

Jane Doe, Chief Financial Officer
Date: _____

(b) Management Report Made at Holding Company Level—Compliance With Designated Laws and Regulations Pertaining to Insider Loans and Dividend Restrictions and No Material Weaknesses in Internal Control Over Financial Reporting

MANAGEMENT REPORT

[*Instruction*—The following illustrative introductory paragraph for the management report is applicable only if the same group of subsidiary institutions of the holding company that are subject to Part 363 are included in all three components of the management report required by Part 363: the statement of management's responsibilities, the report on management's assessment of compliance with the Designated Laws and Regulations pertaining to insider loans and dividend restrictions, and the report on management's assessment of internal control over financial reporting.]

In this management report, the following subsidiary institutions of the BCD Holding Company (the "Company") that are subject to Part 363 are included in the statement of management's responsibilities; the report on management's assessment of compliance with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions; and the re-

port on management's assessment of internal control over financial reporting: [Identify the subsidiary institutions.]

[*Instruction*—The following illustrative introductory paragraph for the management report is applicable if the same group of subsidiary institutions of the holding company that are subject to Part 363 are included in the statement of management's responsibilities and management's assessment of compliance with the Designated Laws and Regulations pertaining to insider loans and dividend restrictions, but only some of the subsidiary institutions in the group are included in management's assessment of internal control over financial reporting.]

In this management report, the following subsidiary institutions of BCD Holding Company (the "Company") that are subject to Part 363 are included in the statement of management's responsibilities and the report on management's assessment of compliance with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions: [Identify the subsidiary institutions.] In addition, the following subsidiary institutions of the Company that are subject to Part 363 are included in the report on management's assessment of internal control over financial reporting: [Identify the subsidiary institutions.]

Statement of Management's Responsibilities

The management of the Company is responsible for preparing the Company's annual financial statements in accordance with generally accepted accounting principles; for establishing and maintaining an adequate internal control structure and procedures for financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report]; and for complying with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions.

Management's Assessment of Compliance With Designated Laws and Regulations

The management of the Company has assessed the Company's compliance with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to dividend restrictions during the fiscal year that ended on December 31, 20XX. Based upon its assessment, management has concluded that the Company complied with the Federal laws and regulations pertaining to insider loans and the Federal and, if applicable, State laws and regulations pertaining to

dividend restrictions during the fiscal year that ended on December 31, 20XX.

Management's Assessment of Internal Control Over Financial Reporting

The Company's internal control over financial reporting is a process effected by those charged with governance, management, and other personnel, designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of reliable financial statements in accordance with accounting principles generally accepted in the United States of America and financial statements for regulatory reporting purposes, *i.e.*, [specify the regulatory reports]. The Company's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the Company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with accounting principles generally accepted in the United States of America and financial statements for regulatory reporting purposes, and that receipts and expenditures of the Company are being made only in accordance with authorizations of management and directors of the Company; and (3) provide reasonable assurance regarding prevention, or timely detection and correction of unauthorized acquisition, use, or disposition of the Company's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies and procedures may deteriorate.

Management assessed the effectiveness of the Company's internal control over financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report], as of December 31, 20XX, based on the framework set forth by the Committee of Sponsoring Organizations of the Treadway Commission in *Internal Control—Integrated Framework*. Based upon its assessment, management has concluded that, as of December 31, 20XX, the Company's internal control over financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report], is effective based on the criteria established in *Internal Control—Integrated Framework*.

Management's assessment of the effectiveness of internal control over financial reporting, including controls over the preparation of regulatory financial statements in accordance with the instructions for the [specify the regulatory report], as of December 31, 20XX, has been audited by [name of auditing firm], an independent public accounting firm, as stated in their report dated March XX, 20XY.

BCD Holding Company

John Doe, Chief Executive Officer

Date: _____

Jane Doe, Chief Financial Officer

Date: _____

7. *Illustrative Cover Letter—Compliance by Holding Company Subsidiaries*. The following illustrative cover letter satisfies the requirements of guideline 3, *Compliance by Holding Company Subsidiaries*, of Appendix A to part 363.

To: (Appropriate FDIC Regional or Area Office) Division of Supervision and Consumer Protection, FDIC, and (Appropriate District or Regional Office of the Primary Federal Regulator(s), if not the FDIC), and

(Appropriate State Bank Supervisor(s), if applicable)

Dear [Insert addressees]:

BCD Holding Company (the "Company") is filing two copies of the Part 363 Annual Report for the fiscal year ended December 31, 20XX, on behalf of its insured depository institution subsidiaries listed in the chart below that are subject to Part 363. The Part 363 Annual Report contains audited comparative annual financial statements, the independent public accountant's report on the audited financial statements, management's statement of responsibilities, management's assessment of compliance with the Designated Laws and Regulations pertaining to insider loans and dividend restrictions, and [if applicable] management's assessment of and the independent public accountant's attestation report on internal control over financial reporting. The chart below also indicates the level (institution or holding company) at which the requirements of Part 363 are being satisfied for each listed insured depository institution subsidiary. [If applicable] The Company's other insured depository institution subsidiaries that are subject to Part 363, which comply with all of the Part 363 annual reporting requirements at the institution level, have filed [or will file] their Part 363 Annual Reports separately.

Institutions subject to Part 363	Audited financial statements	Management's statement of responsibilities	Management's assessment of compliance with designated laws and regulations	Management's internal control assessment	Independent auditor's internal control attestation report
ABC Depository Institution. DEF Depository Institution.	Holding Company Level. Holding Company Level.	Holding Company Level. Institution Level	Holding Company Level. Institution Level	Holding Company Level. Institution Level	Holding Company Level. Institution Level.

If you have any questions regarding the annual report [or reports] of the Company's insured depository institution subsidiaries subject to Part 363 or if you need any further information, you may contact me at 987-654-3210.

BCD Holding Company

Date: _____
[Insert officer's name and title.]

PART 364—STANDARDS FOR SAFETY AND SOUNDNESS

Sec.
364.100 Purpose.
364.101 Standards for safety and soundness.
APPENDIX A TO PART 364—INTERAGENCY GUIDELINES ESTABLISHING STANDARDS FOR SAFETY AND SOUNDNESS
APPENDIX B TO PART 364—INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS

AUTHORITY: 12 U.S.C. 1818 and 1819 (Tenth), 1831p-1; 15 U.S.C. 1681b, 1681s, 1681w, 6801(b), 6805(b)(1).

SOURCE: 60 FR 35685, July 10, 1995, unless otherwise noted.

§364.100 Purpose.

Section 39 of the Federal Deposit Insurance Act requires the Federal Deposit Insurance Corporation to establish safety and soundness standards. Pursuant to section 39, this part establishes safety and soundness standards by guideline.

§364.101 Standards for safety and soundness.

(a) *General standards.* The Interagency Guidelines Establishing Standards for Safety and Soundness prescribed pursuant to section 39 of the Federal Deposit Insurance Act (12 U.S.C. 1831p-1), as set forth as appendix A to this part, apply to all insured state nonmember banks and to state-licensed insured branches of foreign

banks, that are subject to the provisions of section 39 of the Federal Deposit Insurance Act.

(b) *Interagency Guidelines Establishing Information Security Standards.* The Interagency Guidelines Establishing Information Security Standards prescribed pursuant to section 39 of the Federal Deposit Insurance Act (12 U.S.C. 1831p-1), and sections 501 and 505(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801, 6805(b)), and with respect to the proper disposal of consumer information requirements pursuant to section 628 of the Fair Credit Reporting Act (15 U.S.C. 1681w), as set forth in appendix B to this part, apply to all insured state nonmember banks, insured state licensed branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers). The interagency regulations and guidelines on identity theft detection, prevention, and mitigation prescribed pursuant to section 114 of the Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. 1681m(e), are set forth in §§334.90, 334.91, and appendix J of part 334.

[63 FR 55488, Oct. 15, 1998, as amended at 66 FR 8638, Feb. 1, 2001; 69 FR 77619, Dec. 28, 2004; 72 FR 63764, Nov. 9, 2007]

APPENDIX A TO PART 364—INTERAGENCY GUIDELINES ESTABLISHING STANDARDS FOR SAFETY AND SOUNDNESS

TABLE OF CONTENTS

I. Introduction

- A. Preservation of existing authority.
- B. Definitions.

II. Operational and Managerial Standards

- A. Internal controls and information systems.
- B. Internal audit system.
- C. Loan documentation.