The Clearing House®

At the Center of Banking Since 1853®

ANNEX A

U.S. Bank Regulatory Related Matters to be Addressed by the Board or Board Committee Pursuant to Statute, Regulation or Agency Guidance

May 2016

ANNEX A

U.S. Bank Regulatory Related Matters to be Addressed by the Board or Board Committee Pursuant to Statute, Regulation or Agency Guidance

» This Annex A to *The Role of the Board of Directors in Promoting Effective Governance and Safety and Soundness for Large U.S. Banking Organizations* identifies matters to be addressed by boards of directors of U.S. banking organizations that TCH has identified under federal banking laws, regulations and agency guidance statements, including examination procedures or other examination guidance.[1]

» The items enumerated in this Annex A have been promulgated by several different authorities and issued over the course of many years. They include statutory requirements set forth in Title 12 of the U.S. Code, as well as requirements in regulations and agency and interagency guidance statements by the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System ("FRB"), the Federal Deposit Insurance Corporation ("FDIC"), and the Federal Financial Institutions Examination Council ("FFIEC"). This list also includes requirements promulgated by the Consumer Financial Protection Bureau ("CFPB"). The specific agency guidance statements reviewed for each agency are identified further below.

» This Annex A does not include the entire universe of legal requirements that could potentially apply or be applied to a particular institution's board of directors. For example, it does not include requirements that may apply pursuant to federal securities laws, state laws, or stock exchange listing standards. Moreover, this Annex A does not address corporate matters that, in accordance with company policy, practices or charters and in the normal exercise of fiduciary duties, would be presented to the board even if not specifically required by a statute, regulation or agency guidance statement.

» The following agency guidance statements as published through December 31, 2015, were reviewed for inclusion in this list. As noted below, certain of these sources of guidance have been designed for use by agency examiners and generally indicate that examiners are given discretion in how to apply them. Accordingly, their applicability may vary by institution, and this Annex A should not be treated as an enumeration of items applicable to any particular institution or type of institution. Moreover, it is not intended to serve as legal advice.

» **OFFICE OF THE COMPTROLLER OF THE CURRENCY:**

- The Director's Book: The Role of a National Bank Director
- OCC Publication: Red Flags in Board Reports – A Guide for Directors
- OCC Circulars, Bulletins, Handbooks and Journals
- The Comptroller's Handbook
    - *The Comptroller's Handbook is a collection of booklets that contain the concepts and procedures established by the OCC for the examination of national banks. The Foreword to the Handbook states that "OCC examiners consider the risks posed by and the materiality of the areas under examination to decide the scope and additional procedures to be followed. Examiners tailor the examinations to fit the operations of specific banks while fulfilling OCC and statutory requirements."*

» **BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM:**[2]

- Supervision and Regulation Letters
- Bank Holding Company Supervision Manual
    - *The Foreword to the Bank Holding Company Supervision Manual states that it "has been prepared by Federal Reserve supervision personnel to provide guidance to examiners as they conduct on-site inspections*

1 This Annex A identifies matters to be addressed by the boards of directors of national banks, state member banks, state nonmember banks, and bank holding companies. Matters to be addressed at the bank holding company board (rather than bank board) level are specifically noted.

2 This Annex A does not include a review of the FRB Trading and Capital Markets Activities Manual or Consumer Compliance Handbook.

of bank holding companies (BHCs) and their nonbank subsidiaries." Section 1030 (Use of the Manual) further states that "[e]xaminers may exercise a measure of discretion depending upon the characteristics of the organization under inspection."

- Commercial Bank Examination Manual
  - *The Foreword to the Commercial Bank Examination Manual notes that the Manual's goal is "to organize and formalize longstanding examination objectives and procedures that provide guidance to the examiner, and to enhance the quality and consistent application of examination procedures." The Foreword further notes that "[t]he materiality and significance of a given area of bank operations are the examiner's primary considerations in deciding the scope of the examination and the procedures to be performed."*
- Federal Reserve Policy on Payment System Risk

» **FEDERAL DEPOSIT INSURANCE CORPORATION:**

- Pocket Guide for Directors
- Statement Concerning the Responsibilities of Bank Directors and Officers
- Financial Institution Letters
- Risk Management Manual of Examination Policies
  - *Section 1.1 of this Manual states that "[t]he primary purpose of this Manual is to provide policy guidance and direction to the field examiner that should be applied in the risk management examination process," also noting that "[t]he exercise of examiner judgment to determine the scope and depth of review in each functional area is crucial to the success of the risk-focused supervisory process."*
- Credit Card Activities Manual
  - *The Introduction to this Manual states that it "is intended to assist examiners in gaining a broad understanding of the unique characteristics of bank credit card operations," also noting that "examination approaches necessary to assess credit card operations may require augmentation or modification beyond the approaches provided in this manual, depending on circumstances that arise."*
- Credit Card Securitization Manual
  - *The Introduction to this Manual states that it "is intended to assist examiners in understanding and evaluating the credit card securitization process."*
- FDIC Compliance Manual
  - *The Introduction to this Manual states that it is "designed as a reference tool for Compliance examination staff to use when conducting Compliance and Community Reinvestment Act (CRA) examinations and other supervisory activities. The detailed procedures presented in the Manual are not intended to replace sound judgment and discretion on the part of examination staff."*
- Privacy Rule Handbook

» **CONSUMER FINANCIAL PROTECTION BUREAU:**

- Bulletins and Supervisory Highlights
- CFPB Supervision and Examination Manual

» **INTERAGENCY AND FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL:**

- Booklets that Comprise the FFIEC Technology Examination Handbook
  - *The FFIEC's "Handbook Overview" presentation notes that "[a]lthough the booklets are intended for use by a wide range of audiences, the content is written at a level appropriate for a midlevel IT examiner. Examiners will*

target the workprogram procedures based on the risk in specific examination environments."

- BSA/AML Examination Manual
    - *The Introduction to this Manual states that it "provides guidance to examiners for carrying out BSA/AML and Office of Foreign Assets Control (OFAC) examinations." The Introduction further notes that "[i]n order to effectively apply resources and ensure compliance with BSA requirements, the [M]anual is structured to allow examiners to tailor the BSA/AML examination scope and procedures to the specific risk profile of the banking organization."*
- Interagency and FFIEC Guidance Policy Statements

For each category of items (*i.e.*, statutes, regulations or agency guidance statements), this Annex A categorizes the items by the applicable agency. Where regulations are substantively identical across multiple agencies, this list does not repeat the complete description for each agency; rather it includes the full description for one agency, and the corresponding items for the other agencies are described by reference.

I. Matters to be Addressed by Board of Directors Pursuant to Statute or Regulation

A. TITLE 12, UNITED STATES CODE

1. National Bank Act

» Appoint a president, vice president, cashier, and other officers; define their duties; require bonds of them and fix the penalty thereof; dismiss such officers or any of them at pleasure; and appoint others to fill their places. 12 U.S.C. 24.

» Prescribe bylaws consistent with law. 12 U.S.C. 24.

» Contribute to community funds or charitable, philanthropic, or benevolent instrumentalities in such sums as the board of directors deems expedient and in the banking association's interest. 12 U.S.C. 24.

» Conversion of state charter to national banking association charter; execution of organization certificate and articles of association and other documents necessary to convert. 12 U.S.C. 35.

» Issuance of preferred stock. 12 U.S.C. 51a.

» Sale of a shareholder's stock at public auction to enforce payment of a deficiency assessment imposed on the shareholder. 12 U.S.C. 55.

» Declaration of a dividend. 12 U.S.C. 60; *see also* Section 25A(18) of the Federal Reserve Act, 12 U.S.C. 626, with respect to Edge corporations.

» Appointment of a director to fill a vacancy in the board. 12 U.S.C. 74.

» Designation of day to elect directors when regularly scheduled election is not held for some reason. 12 U.S.C. 75.

» Designation of a director other than the bank president to be chairman of the board. 12 U.S.C. 76.

» Surrender trust powers. 12 U.S.C. 92a.

» Designation of bank officer to sign certification of accuracy of the bank's call report; the correctness of the report shall be attested by the signatures of at least three of the bank's directors, with the declaration that the report has been examined by them and to the best of their knowledge and belief is true and correct. 12 U.S.C. 161.

» Supervision of liquidator of the bank. 12 U.S.C. 181.

» Notice to public and OCC that a vote has been taken for bank to go into liquidation. 12 U.S.C. 182.

» OCC may appoint a conservator of the bank upon vote of the bank's board. 12 U.S.C. 203.

» Various matters related to bank mergers, conversions and dissenting shareholders. 12 U.S.C. 214a, 215, 215a, 215a-1, 215a-3; *see also* Section 25A(21) of the Federal Reserve Act, 12 U.S.C. 629, with respect to the conversion of a state corporation into an Edge corporation.

- Approve a plan of conversion, merger, or consolidation.
- Determine the par price for the shares of dissenting shareholders sold at auction after those shareholders request payment in a consolidation or merger.
- Execute all documents and papers required to convert into a federal corporation.

» Reorganization so as to become a subsidiary of a bank holding company or of a company that will, upon

consummation of such reorganization, become a bank holding company. 12 U.S.C. 215a-2.

2. Federal Reserve Act

» Authorization of the purchase or acquisition of securities even though a principal underwriter of the securities is an affiliate of the bank; this can be done only if the purchase has been approved, before such securities are initially offered for sale to the public, by a majority of the bank's board based on a determination that the purchase is a sound investment irrespective of the fact that an affiliate of the bank is a principal underwriter of the securities. 12 U.S.C. 371c-1 (Section 23B of the Federal Reserve Act).

» Receipt of reports of certain loans to executive officers of the bank. 12 U.S.C. 375a.

» Authorization of loans to an executive officer, director or principal shareholder, or to any related interest of such a person, that would case a statutorily-imposed aggregate credit limit to be exceeded, subject to certain conditions. 12 U.S.C. 375b.

3. Federal Deposit Insurance Act

» The signatures declaring that a call report is accurate must be attested by at least two directors; their attestation must state that the report has been examined by them and to the best of their knowledge and belief is true and correct. 12 U.S.C. 1817(a)(3).

- *See also* 12 U.S.C. 161 (National Bank Act), which requires the signatures of three directors for call reports filed by a national bank.

» The board of directors may consent to the FDIC's appointment of a conservator or receiver to the insured depository institution. 12 U.S.C. 1821(c)(5).

» The board or its loan committee must approve any agreement which tends to diminish or defeat the interest in an asset of the FDIC as conservator or receiver, in order for that agreement to be valid against the FDIC. 12 U.S.C. 1823(e).

» Corporation may assist an acquisition or merger of insured banks in danger of default only if the board of directors or trustees of each insured bank in danger of default which is being acquired has requested in writing that the FDIC assist the acquisition or merger. 12 U.S.C. 1823(f).

» An insured depository institution may not purchase an asset from, or sell an asset to, an executive officer, director, or principal shareholder of the institution, or any related interest of such person, unless: (a) the transaction is on market terms; and (b) if the transaction represents more than 10% of the capital stock and surplus of the institution, the transaction has been approved by a majority of the members of the board of directors who do not have an interest in the transaction. 12 U.S.C. 1828(z).

» Each insured depository institution shall have an independent audit committee entirely made up of outside directors who are independent of management of the institution, and who satisfy any specific requirements the FDIC may establish. 12 U.S.C. 1831m(g)(1).

- The appropriate federal banking agency may, by order or regulation, permit an institution's audit committee to be made up of less than all, but no fewer than a majority of, outside directors, 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 committee. 1831m(g)(1)(D).

4. Dodd-Frank Wall Street Reform and Consumer Protection Act

» An institution that has received TARP funds must establish a board compensation committee comprised entirely of independent directors to review employee compensation plans. The board compensation committee shall meet at least semiannually to discuss and

evaluate employee compensation plans in light of an assessment of any risk posed to the TARP recipient from such plans. In the case of any TARP recipient, the common or preferred stock of which is not registered pursuant to the Securities Exchange Act of 1934, and that has received $25,000,000 or less of TARP assistance, the duties of the Board Compensation Committee under this subsection shall be carried out by the board of directors of such TARP recipient. 12 U.S.C. 5221(c), as implemented by 31 C.F.R. 30.4, generally applicable as long as TARP obligations remain outstanding.

» The board of directors of a TARP recipient must establish a company-wide policy regarding excessive or luxury expenditures. 12 U.S.C. 5221(d), as implemented by 31 C.F.R. 30.12, generally applicable as long as TARP obligations remain outstanding.

» A publicly-traded bank holding company with assets of $10 billion or more must establish a risk committee that is chaired by an independent director and has at least one member with sufficient risk management expertise. 12 U.S.C. 5365(h), as implemented by 12 C.F.R. 252.22 and 252.33 (described further below).

» The FRB may not object to a waiver by a mutual holding company of the right to receive any dividend declared by a subsidiary of the mutual holding company if:

- the board of directors of the mutual holding company expressly determines that a waiver of the dividend by the mutual holding company is consistent with the fiduciary duties of the board of directors to the mutual members of the mutual holding company;
- the waiver would not be detrimental to the safe and sound operation of the savings association; and
- the mutual holding company has, prior to December 1, 2009: reorganized into a mutual holding company; issued minority stock either from its midtier stock holding company or its subsidiary stock savings association; and waived dividends it had a right to receive from the subsidiary stock savings association. 12 U.S.C. 1467a(o) (Home Owners' Loan Act, as amended by the Dodd-Frank Act).

B. TITLE 12, CODE OF FEDERAL REGULATIONS - OCC REGULATIONS

» According to the OCC's Capital Adequacy Standards for National Banks, the board of directors of an advanced approaches national bank must approve the advanced approaches implementation plan. 12 C.F.R. 3.121(b)(1)(viii).

- In addition, the board or a designated committee thereof must:
  - *Review the effectiveness of, and approve, the bank's advanced systems at least annually. 12 C.F.R. 3.122(i)(2).*
    - *Advanced systems* means an advanced approaches national bank's advanced internal ratings-based systems, operational risk management processes, operational risk data and assessment systems, operational risk quantification systems, and, to the extent used by the national bank, the internal models methodology, advanced CVA approach, double default excessive correlation detection process, and internal models approach for equity exposures. 12 C.F.R. 3.101(b).
  - *Receive reports on operational risk exposures. 12 C.F.R. 3.122(g)(1)(iii).*
  - *Receive reports at least annually from the internal audit function on the effectiveness of the controls supporting the national bank's advanced systems. 12 C.F.R. 3.122(i)(5).*
- In addition, if the national bank has total consolidated assets of $50 billion or more (whether or not it is an advanced approaches national bank), it must have a formal disclosure policy approved by the board of directors that addresses its approach for determining its capital-related disclosures (including, if applicable, as noted

below, market risk disclosures) and that also addresses the associated internal controls and disclosure controls and procedures. 12 C.F.R. 3.62; 3.172; 3.212.

- *The board of directors and senior management are responsible for establishing and maintaining an effective internal control structure over financial reporting, including the disclosures required by these capital regulations, and must ensure that appropriate review of the disclosures takes place. Id.*

- *A bank is not required to comply with these disclosure requirements if it is a consolidated subsidiary of a bank holding company or a depository institution that is subject to these requirements or of a non-U.S. banking organization that is subject to comparable public disclosure requirements in its home jurisdiction. Id.*

- If a national bank is subject to the market risk capital rule (*e.g.*, it has aggregate trading assets and trading liabilities of at least $1 billion or 10 percent of total assets), at least annually the internal audit function must report its findings to the board of directors (or a committee thereof) regarding the effectiveness of the controls supporting the bank's market risk measurement systems, including the activities of the business trading units and independent risk control unit, compliance with policies and procedures, and calculation of the bank's measures for market risk. 12 C.F.R. 3.203(d)(4). 12 C.F.R. Part 3, Appendix B.

  - *In addition, the bank must maintain a formal disclosure policy approved by the board of directors that addresses the bank's approach for determining its market risk disclosures. The board of directors and senior management must ensure that appropriate verification of the disclosures takes place and that effective internal controls and disclosure controls and procedures are maintained; the board of directors and senior management are responsible for establishing and maintaining an effective internal control structure over financial reporting, including the disclosures required by this section. 12 C.F.R. 3.212(b). 12 C.F.R. Part 3, Appendix B.*

  - A bank is not required to comply with these disclosure requirements if it is a consolidated subsidiary of a bank holding company or a depository institution that is subject to these requirements or of a non-U.S. banking organization that is subject to comparable public disclosure requirements in its home jurisdiction. *Id.*

» Approve a plan to reorganize as subsidiary of a bank holding company. 12 C.F.R. 5.32.

» Declare and pay dividends from undivided profits, and approve transfer of "surplus surplus" from capital surplus to undivided profits and thus made available to pay dividends, subject to certain limits. 12 C.F.R. 5.64.

» Declare property dividends, with the approval of the OCC. 12 C.F.R. 5.66.

» After holding OREO for a year, the bank shall state, by resolution of the board of directors or an appropriately authorized bank official or subcommittee of the board, definite plans for its use. 12 C.F.R. 7.100(d).

» Increase the number of the bank's directors or fill a vacancy, subject to certain limits. 12 C.F.R. 7.2007.

» Manage or direct the management of the business and affairs of the bank (refers to OCC published guidance for additional information regarding the responsibilities of bank directors). 12 C.F.R 7.2010.

» Determine the amount of adequate fidelity bond coverage. 12 C.F.R. 7.2013.

» Assign some or all of the duties previously performed by the bank's cashier to its president, chief executive officer, or any other officer. 12 C.F.R. 7.2015.

» Fix a record date for determining the shareholders entitled to notice of, and to vote at, any meeting of shareholders. 12 C.F.R. 7.2016.

» Review and schedule the bank's banking hours. 12 C.F.R. 7.3000.

» Thoroughly review the OCC's exam report of the bank. 12 C.F.R. 7.4000.

» Directly, or through a designee, assign functions to fiduciary officers and employees. 12 C.F.R. 9.2.

» A national bank's fiduciary activities shall be managed by or under the direction of its board of directors. The board, in discharging this duty, may assign any function related to the exercise of fiduciary powers to any director, officer, employee or committee thereof. 12 C.F.R. 9.4.

» At least once each year, a national bank's fiduciary audit committee must arrange for a suitable audit of all significant fiduciary activities, under the audit committee's direction. Alternatively, the bank may adopt a continuous audit system under which the bank arranges for a discrete audit (by internal or external auditors) of each significant audit activity, under the direction of its fiduciary audit committee. The bank shall note the results of the audit in the minutes of the board of directors. A bank's fiduciary audit committee must consist of a committee of the bank's directors or an audit committee of an affiliate of the bank; however in either case, the committee: (a) must not include any officers of the bank or an affiliate who participate significantly in the administration of the bank's fiduciary activities; and (b) must consist of a majority of members who are not also members of any committee to which the board of directors of the bank has delegated power to manage and control the fiduciary activities of the bank. 12 C.F.R. 9.9.

» The board of directors must appoint not fewer than two of the bank's fiduciary officers or employees in whose joint custody or control the bank shall place assets of fiduciary accounts. 12 C.F.R. 9.13.

» A national bank may not permit any officer or employee to retain any compensation for action as a co-fiduciary with the bank in the administration of a fiduciary account, except with the specific approval of the bank's board of directors. 12 C.F.R. 9.15.

» A bank seeking to surrender its fiduciary powers must do so pursuant to a resolution of the board of directors. 12 C.F.R. 9.17.

» The bank shall establish and administer each collective investment fund pursuant to a written plan approved by a resolution of the bank's board of directors or by a committee authorized by the board. 12 C.F.R. 9.18(b)(1).

» At least once each 12-month period, the bank administering a collective investment fund shall arrange for an audit of the fund by auditors responsible only to the board of directors. 12 C.F.R. 9.18(b)(6).

» Minimum Security Devices and Procedures. It is the responsibility of the bank's board of directors to comply with the OCC regulation on minimum security devices and procedures (12 C.F.R. Part 21, Subpart A, issued pursuant to Section 3 of the Bank Protection Act of 1968, 12 U.S.C. 1882), and ensure that a security program which meets the requirements of the regulation is developed and implemented by the bank for its main office and branches. 12 C.F.R. 21.1.

- The bank's board of directors must appoint a security officer, who shall have the authority, subject to the approval of the board of directors, to develop and administer a written security program. 12 C.F.R. 21.2.

- The bank's security officer must report at least annually to the bank's board of directors on the effectiveness of the security program, and the substance of the report must be reflected in the relevant board meeting minutes. 12 C.F.R. 21.4.

» Whenever a bank files a suspicious activity report, the bank's management shall promptly notify the board of directors, or a committee of the directors or executive

officers designated by the board to receive the notice. 12 C.F.R. 21.11(h)(1).

- If a bank files a suspicious activity report and the suspect is a director or executive officer, the bank may not notify the suspect, pursuant to 31 U.S.C. 5318(g)(2), but must notify all directors who are not suspects. 12 C.F.R. 21.11(h)(2).

» The board of directors must approve the bank's Bank Secrecy Act written compliance program. 12 C.F.R. 21.21.

» According to 12 C.F.R. Part 30, Appendix A – Interagency Guidelines Establishing Standards for Safety and Soundness, a bank should:

- Have an internal audit system that, among other things, provides for review of its effectiveness by the bank's audit committee or board of directors;
- Establish and maintain prudent credit underwriting practices that, among other things, include a system of independent, ongoing credit review and appropriate communication to management and the board of directors;
- Provide for periodic reporting to management and the board of directors regarding interest rate risk with adequate information for management and the board of directors to assess the level of risk;
- Establish and maintain a system to identify problem assets and prevent deterioration in those assets that, among other things, includes providing periodic asset reports with adequate information for management and the board of directors to assess the level of asset risk; and
- Establish and maintain a system to evaluate and monitor earnings and ensure that earnings are sufficient to maintain adequate capital and reserves, including, among other things, providing periodic earnings reports with adequate information for management and the board of directors to assess earnings performance.

» According to 12 C.F.R. Part 30, Appendix B – Interagency Guidelines Establishing Information Security Standards, the board of directors, or an appropriate committee of the board, shall (a) approve the bank's written information security program; (b) oversee the development, implementation, and maintenance of the bank's information security program, including assigning specific responsibility for its implementation and reviewing reports from management; and (c) receive reports at least annually on the status of the program and compliance with these guidelines.

» According to 12 C.F.R. Part 30, Appendix D – OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches:

- This guidance generally applies to national banks, insured federal savings associations or insured federal branches with $50 billion or more in total assets ("Covered Banks"). However, it can apply to a national bank, insured federal savings association or insured federal branch with assets below this threshold if (i) such entity's parent company controls at least one Covered Bank or (ii) the OCC determines such entity's operations are highly complex or otherwise present a heightened risk such as to warrant application of this guidance.
- The board of directors or its risk committee should approve a formal, written risk governance framework that is designed by independent risk management.
  - *The definition of "independent risk management" requires that the board or its risk committee approves all decisions regarding the appointment or removal of the Chief Risk Executive(s) (including annual compensation and salary adjustments), and that each Chief Risk Executive has unrestricted access to the board and its committees to address risks and issues.*
  - *The risk governance framework should include delegations of authority from the board of directors to manage-*

ment committees and executive officers as well as the risk limits established for material activities.

- *Among other things, the framework should require review and approval of the risk appetite statement (which should include both qualitative components and quantitative limits, as set forth in the guidelines) by the board or its risk committee at least annually or more frequently, as necessary.*

- *The board or its risk committee should approve any significant changes to the framework and monitor compliance with the framework.*

- The board should actively oversee the Covered Bank's risk-taking activities and hold management accountable for adhering to the risk governance framework.

  - *In providing active oversight, the board may rely on risk assessments and reports prepared by independent risk management and internal audit to support the board's ability to question, challenge, and when necessary, oppose recommendations and decisions made by management that could cause the Covered Bank's risk profile to exceed its risk appetite or jeopardize its safety and soundness.*

  - *The board or its risk committee should receive certain communications and reports specified in the guidelines, including with respect to material risks identified by independent risk management and significant instances where a front line unit or the CEO is not adhering to the risk governance framework.*

  - *Among other things, the risk governance framework should require reporting to the board or its risk committee at least quarterly on the monitoring by independent risk management of the national bank's, insured federal savings association's or insured federal branch's risk profile relative to its risk appetite and compliance with concentration risk limits.*

  - *To promote its oversight role, at least two members of the board should meet the independence criteria specified in the guidelines.*

- The definition of "internal audit" requires that the Chief Audit Executive have unrestricted access to the board's audit committee to address risks and issues; the audit committee review and approve internal audit's overall charter and audit plans; the audit committee approve all decisions regarding the appointment or removal and annual compensation and salary adjustment of the Chief Audit Executive; and the audit committee or the CEO oversee the Chief Audit Executive's administrative activities.

  - *The audit committee should receive communications and reports regarding significant changes to the audit plan; conclusions, material issues (including root causes) and recommendations from audit work carried out under the audit plan; and significant instances where front line units or independent risk management are not adhering to the risk governance framework.*

- The board of directors should evaluate and approve the strategic plan and monitor management's efforts to implement the strategic plan at least annually.

- The board or an appropriate committee of the board should appoint the CEO and appoint or approve the appointment of a Chief Audit Executive and one or more Chief Risk Executives; review and approve a written talent management program; and require management to assign individuals specific responsibilities within the talent management program, and hold those individuals accountable for the program's effectiveness.

- The board should establish and adhere to a formal, ongoing training program for all directors. This program should consider the directors' knowledge and experience and the covered bank's risk profile. The program should include, as appropriate, training on: (1) complex products, services, lines of business, and risks that have a significant impact on the covered bank; (2) laws, regulations, and supervisory requirements applicable to the covered bank; and (3) other topics identified by the board of directors.

- The board should conduct an annual self-assessment that includes an evaluation of its effectiveness in meeting the standards set forth in the guidelines.

» Extensions of credit to executive officers, directors, principal shareholders, or related interests of those persons (12 C.F.R. 31.2). *See* description in corresponding FRB regulations discussed below.

» Approve any use of supplemental lending limits for residential real estate, small business, and small farm loans. 12 C.F.R. 32.7.

» According to 12 C.F.R. 34.62 and 12 C.F.R. Part 34, Appendix A to Subpart D – Interagency Guidelines for Real Estate Lending Policies for insured national banks:

- The bank's real estate lending policies (including, among other things, the bank's real estate appraisal and evaluation program) must be reviewed and approved by the board of directors at least annually.

- Bank management must monitor the bank's real estate loan portfolio and provide timely and adequate reports to its board of directors.

  - *The aggregate amount of loans in excess of supervisory loan-to-value limits should be reported at least quarterly to the bank's board of directors.*

  - *The board of directors is responsible for establishing standards for the review and approval of exception loans.*

  - *The bank must individually report exception loans of a significant size to its board of directors.*

» According to 12 C.F.R. 41.90(e)(1) and 12 C.F.R. Part 41, Appendix J – Interagency Guidance on Identity Theft Detection, Prevention and Mitigation, the board or an appropriate committee thereof must approve an initial written program designed to detect, prevent, and mitigate identity theft in connection with covered accounts, which include accounts offered or maintained primarily for personal, family or household purposes, that involve or are designed to permit multiple payments or transactions (such as credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts or savings accounts) or any other accounts offered or maintained for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft.

- The board or an appropriate committee thereof, or a designated employee at the level of senior management must be involved in the oversight, development, implementation and administration of the program.

- The board of directors, a board committee or designated senior management employee should oversee the written program, including assigning specific responsibility for the program's implementation, reviewing reports prepared by staff regarding compliance, and approving material changes to the program as necessary to address changing identity theft risks.

- Staff responsible for development, implementation, and administration of the program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the institution.

» According to the regulations implementing the Volcker Rule, at 12 C.F.R. Part 44:

- The board or an appropriate committee of the board must approve a written Volcker Rule compliance program. 12 C.F.R. Part 44, Appendix B, at III.a.1.

- The board must review the effectiveness of the Volcker Rule compliance program. *Id*. at I.a.4.

- The board of directors, or similar corporate body, and

senior management are responsible for setting and communicating an appropriate culture of compliance with the Volcker Rule and ensuring the adoption of appropriate policies. *Id*. at III.a.4.

- The board of directors or similar corporate body (such as a designated committee of the board or an equivalent governance body) must ensure that senior management is fully capable, qualified, and properly motivated to manage compliance with the Volcker Rule in light of the organization's business activities and the expectations of the board of directors. *Id*. at III.a.4.

- The board of directors or similar corporate body must also ensure that senior management has established appropriate incentives and adequate resources to support compliance with this part, including the implementation of a compliance program into management goals and compensation structures across the banking entity. *Id*. at III.a.4.

- Written policies and procedures must provide for prompt notification to the board of directors of any material weakness or significant deficiencies in the design or implementation of the compliance program. *Id*. at II.a.7 and II.b.6.

» According to the regulations implementing the requirement under Section 165 of the Dodd-Frank Act to conduct annual company-run stress tests, at 12 C.F.R. Part 46:

- The board of directors, or a committee thereof, of an institution with greater than $10 billion in total assets must approve and review the policies and procedures of the institution's stress testing processes as frequently as economic conditions or the condition of the institution may warrant, but no less than annually. 12 C.F.R. 46.6(c)(2).

- The board of directors and senior management must be provided with a summary of the stress test results. *Id*.

- The board of directors and senior management must consider the results of the company-run stress tests in the normal course of business, including but not limited to the institution's capital planning, assessment of capital adequacy, and risk management practices. 12 C.F.R. 46.5(d).

C. TITLE 12, CODE OF FEDERAL REGULATIONS - FDIC REGULATIONS

» Under the FDIC's prompt corrective action regulations, undercapitalized insured state nonmember banks must submit applications to the FDIC to engage in certain activities; such applications must be authorized by the board of directors. 12 C.F.R. 303.200 – 303.207.

» Approve any proposal (which must also receive approval from the FDIC) to reduce the amount or retire any part of the institution's common or preferred stock, or to retire any part of its capital notes or debentures. 12 C.F.R. 303.241.

» Approve application to resume FDIC insured status if status had been previously terminated. 12 C.F.R. 303.247.

» Board of directors' approval is one requirement that must be met for an insured depository institution to release the report of an examination conducted in whole or in part by the FDIC to a majority shareholder. 12 C.F.R. 309.6.

» Annual Company-Run Stress Tests, applicable to state nonmember banks with greater than $10 billion in total assets (12 C.F.R. Part 325, Subpart C). *See* description in corresponding OCC regulations discussed above.

» Capital Adequacy Standards for State Nonmember Banks (12 C.F.R. Part 325, Appendix D); *see also* 12 C.F.R. 324.62(b), 324.121(b)(viii), 324.122(i)(2), 324.172(b), 324.204(d)(4), 324.212(b). *See* description in corresponding OCC regulations discussed above.

» Minimum Security Devices and Procedures (12 C.F.R. Part 326). *See* description in corresponding OCC regulations discussed above. The annual report of the bank's

security officer to the board also must cover the implementation and administration of the plan (in addition to its effectiveness). 12 C.F.R. 326.4.

» Approve a written program for compliance with the Bank Secrecy Act. 12 C.F.R. 326.8.

» Identity theft prevention program (12 C.F.R. 334.90; 12 C.F.R. Part 334, Appendix J). *See* description in corresponding OCC regulations discussed above.

» Extensions of credit to executive officers, directors, principal shareholders, or related interests of those persons (12 C.F.R. 337.3). *See* description in corresponding FRB regulations discussed below.

» Volcker Rule (12 C.F.R. Part 351). *See* description in corresponding OCC regulations discussed above.

» Whenever a bank files a suspicious activity report, the bank's management shall promptly notify the board of directors, or a committee thereof. 12 C.F.R. 353.3.

» An insured depository institution or depository institution holding company may make or agree to make reasonable indemnification payments to an institution-affiliated party ("IAP") if: (1) the insured depository institution's or depository institution holding company's board of directors, in good faith, determines in writing after due investigation and consideration that the IAP acted in good faith and in a manner he/she believed to be in the best interests of the institution; (2) the insured depository institution's or depository institution holding company's board of directors, respectively, in good faith, determines in writing after due investigation and consideration that the payment of such expenses will not materially adversely affect the institution's or holding company's safety and soundness; (3) the indemnification payments do not constitute prohibited indemnification payments; and (4) the IAP agrees in writing to reimburse the insured depository institution or depository institution holding company, to the extent not covered by permissible insurance, for payments made in the event that the IAP does not prevail. 12 C.F.R. 359.5.

  - An IAP requesting indemnification payments shall not participate in any way in the board's discussion and approval of such payments; provided, however, that such IAP may present his/her request to the board and respond to any inquiries from the board concerning his/her involvement in the circumstances giving rise to the administrative proceeding or civil action.

  - Certain procedures apply in the event that a majority of the members of the board of directors are named as respondents in an administrative proceeding or civil action and request indemnification.

» The board of directors of the bank or its loan committee (as reflected in the minutes of a meeting of the board or committee) shall approve certain securitization agreements relating to the transfer of financial assets. 12 C.F.R. 360.6.

» The board of directors of an insured depository institution with $50 billion or more in total assets must approve the institution's resolution plan prior to its submission each year to the FDIC. (12 C.F.R. 360.10(c)(3)).

» If a bank seeks to engage in underwriting securities that are not permissible for a national bank under 12 U.S.C. 24 (Seventh) through a majority-owned subsidiary in existence prior to November 12, 1999 (rather than through a financial subsidiary), the bank may not knowingly purchase, as principal or fiduciary during the existence of any underwriting or selling syndicate, any securities underwritten by the majority-owned subsidiary unless the purchase is approved by the board of directors before the securities are initially offered for sale. 12 C.F.R. 362.4.

» Each insured depository institution shall establish an independent audit committee of its board of directors; duties 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 12 C.F.R. Part 363.

- The members of such committee of each insured depository institution with total assets of $1 billion or more shall be outside directors who are independent of management of the institution.

- The members of the audit committee of each insured depository institution with total assets of $500 million or more but less than $1 billion shall be outside directors, the majority of whom shall be independent of management.

- The audit committee of any insured depository institution that has total assets of more than $3 billion 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 audit committee shall not include any members who are large customers of the subsidiary institution.

» In performing its duties with respect to the appointment of the institution's independent public accountant, the audit committee must ensure that engagement letters and any related agreements with the independent public accountant for services to be performed under 12 C.F.R. Part 363 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. 12 C.F.R. 363.5.

» Appendix A to 12 C.F.R. Part 363 provides further guidance on audit committees:

- Multi-tiered holding companies may satisfy all requirements of Part 363 at any level.

- The independent public accountant who audits an institution's financial statements 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.

- The insured depository institution's audit committee shall review with management and the independent public accountant who audits the bank the basis for (a) the internal control reports required by section 36 of the FDI Act; (b) the independent auditor's reports on the institution's internal control reports; and (c) the independent audit required by section 36. The internal control reports the audit committee must review include a report signed by the chief executive officer and the chief accounting officer or financial officer of the institution which contains:

  - *(a) a statement of the management's responsibilities for (i) preparing financial statements, (ii) establishing and maintaining an adequate internal control structure and procedures for financial reporting; and (iii) complying with the laws and regulations relating to safety and soundness which are designated by the FDIC and appropriate federal banking agency; and*

  - *(b) an assessment, as of the end of the institution's most recent fiscal year, of (i) the effectiveness of such internal control structure and procedures; and (ii) the institution's compliance with the laws and regulations relating to safety and soundness which are designated by the FDIC and the appropriate federal banking agency.*

» Interagency Guidelines Establishing Standards for Safety and Soundness (12 C.F.R. Part 364, Appendix A). *See* description in corresponding OCC regulations discussed above.

» Interagency Guidelines Establishing Standards for Safeguarding Customer Information (12 C.F.R. Part 364, Appendix B). *See* description in corresponding OCC regulations discussed above.

» Interagency Guidelines for Real Estate Lending Policies (12 C.F.R. Part 365, Appendix A to Subpart A) and 12 C.F.R. 365.2. *See* description in corresponding OCC regulations discussed above.

» The board of directors of a bank holding company with $50 billion or more in total assets must approve the bank holding company's resolution plan (which is required under Section 165(d) of the Dodd-Frank Act and separate from the insured depository institution plan described above) prior to its submission each year to the FRB and the FDIC. 12 C.F.R. 381.3(e).

- With respect to a foreign-based company required to submit a resolution plan under the regulation (*e.g.*, a foreign bank or company that is a bank holding company or is treated as a bank holding company under section 8(a) of the International Banking Act of 1978), the resolution plan must be approved by the board of directors or by a delegee acting under the express authority of the board of directors.

D. TITLE 12, CODE OF FEDERAL REGULATIONS - FEDERAL RESERVE BOARD REGULATIONS

1. Regulation F – Limitations on Interbank Liabilities (12 C.F.R. Part 206, applicable to all insured depository institutions)

» A bank's written policies and procedures to prevent excessive exposure to any individual correspondent shall be reviewed and approved by the bank's board of directors at least annually. 12 C.F.R. 206.3.

» A bank may rely on another party to assess the financial condition of or select a correspondent, provided the bank's board of directors has reviewed and approved the general assessment or selection criteria used by the other party. 12 C.F.R. 206.3.

2. Regulation H – Membership of State Banking Institutions in the Federal Reserve System (12 C.F.R. Part 208, applicable to state member banks)

» Approve the transfer of capital surplus in excess of that required by law to the bank's undivided profits account, making the funds available for the payment of dividends. 12 C.F.R. 208.5.

» Minimum Security Devices and Procedures (12 C.F.R. 208.61). *See* description in corresponding OCC regulations discussed above. The annual report of the bank's security officer to the board also must cover the implementation and administration of the plan (in addition to its effectiveness). 12 C.F.R. 208.61(d).

» Whenever a bank files a suspicious activity report, the bank's management shall promptly notify the board of directors, or a committee thereof. 12 C.F.R. 208.62(h).

» Approve (and note in the relevant board meeting minutes) a written program for compliance with the Bank Secrecy Act. 12 C.F.R 208.63(b).

» Interagency Guidelines for Real Estate Lending Policies (12 C.F.R. Part 208, Appendix C) and 12 C.F.R. 208.51. *See* description in corresponding OCC regulations described above.

» Interagency Guidelines Establishing Standards for Safety and Soundness (12 C.F.R. Part 208, Appendix D-1). *See* description in corresponding OCC regulations described above.

» Interagency Guidelines Establishing Information Security Standards (12 C.F.R. Part 208, Appendix D-2). *See* description in corresponding OCC regulations

described above.

3. Regulation K – International Banking Operations (12 C.F.R. Part 211, with respect to the requirement noted below, applicable to Edge and agreement corporations)

» The board of directors of an Edge or agreement corporation shall approve the BSA/AML compliance program and note the approval in the meeting minutes. 12 C.F.R. 211.5(m)(1).

4. Regulation O – Loans to Executive Officers, Directors, and Principal Shareholders of Member Banks (12 C.F.R. Part 215, applicable to member banks and as also made specifically applicable to state nonmember banks and to national banks under 12 C.F.R. 337.3 and 12 C.F.R. Part 31, respectively)

» Pursuant to the FRB's Regulation O, 12 C.F.R. Part 215, the board of directors is required to act or receive reports on various matters in connection with extensions of credit granted to the executive officers, directors or principal shareholders of the bank or an affiliate, or to related interests of those persons.

- Board approval generally is required for any such extension of credit that, when aggregated with the amount of all other extensions of credit to the relevant person and to all related interests of that person, would exceed certain amounts prescribed by regulation. 12 C.F.R. 215.4(b).

- Any extension of credit to an executive officer of the bank must be promptly reported to the bank's board of directors. 12 C.F.R. 215.5(d).

- Each executive officer or director of a bank that is not publicly traded must report annually to the board of directors the outstanding amount of any credit extended to that person that is secured by shares of the bank. 12 C.F.R. 215.10.

- The board of directors of a bank with deposits of less than $100 million may resolve annually to increase the applicable aggregate lending limit for all such transactions. 12 C.F.R. 215.4(d)(2).

- The regulation's recordkeeping requirements require the bank to survey its executive officers, directors and principal shareholders in order to identify persons that are subject to the regulation's restrictions (namely, any related interests of those persons). 12 C.F.R. 215.8.

5. Regulation Q – Capital Adequacy (12 C.F.R. Part 217, applicable to bank holding companies and state member banks)

» Capital Adequacy Guidelines for State Member Banks and Bank Holding Companies: Internal-Ratings-Based and Advanced Measurement Approaches (12 C.F.R. Part 217, Subpart E); *see also* 12 C.F.R. 217.62(b)). *See* description in corresponding OCC regulations discussed above.

6. Regulation V – Fair Credit Reporting (12 C.F.R. Part 222, applicable to state member banks and bank holding companies)

» Identity theft prevention program (12 C.F.R. 222.90; 12 C.F.R. Part 222, Appendix J). *See* description in corresponding OCC regulations above.

7. Regulation W – Transactions between Member Banks and their Affiliates (12 C.F.R. Part 223, applicable to member banks, and as made applicable to state nonmember banks by 12 U.S.C. 1828(j))

» A bank's ability to rely on certain exemptions from the requirements of Sections 23A or 23B of the Federal Reserve

Act (including with respect to a the renewal of a participation in a problem loan originated by an affiliate, certain internal corporate reorganization transactions, and the purchase of as security underwritten by an affiliate) are predicated on, among other things, approval by the bank's board of directors. 12 C.F.R. 223.15(b), 223.41, 223.53.

8. Regulation Y – Bank Holding Companies and Change in Bank Control (12 C.F.R. Part 225, applicable to bank holding companies)

» Each executive officer or director of a bank holding company the shares of which are not publicly traded shall report annually to the board of directors of the bank holding company the outstanding amount of any credit that was extended to the executive officer or director and that is secured by shares of the bank holding company. 12 C.F.R. 225.4.

» The board of directors (or a designated committee thereof) of a bank holding company that is required to file a capital plan with the FRB and appropriate Federal Reserve Bank (e.g., a top-tier bank holding company with at least $50 billion in total assets) must, at least annually and prior to submission of the capital plan: (A) review the robustness of the bank holding company's process for assessing capital adequacy; (B) ensure that any deficiencies in the bank holding company's process for assessing capital adequacy are appropriately remedied; and (C) approve the bank holding company's capital plan. 12 C.F.R. 225.8(e)(1)(iii).

» Notice procedure for the establishment of a one-bank holding company requires a certification of certain matters by the notificant's board of directors. 12 C.F.R. 225.17.

» If a bank holding company or nonbank subsidiary that engages in futures, forward and option contracts on U.S. Government and agency securities and money market instruments is taking or intends to take positions in financial contracts, the company's board of directors should approve prudent written policies and establish appropriate limitations to insure that financial contract activities are performed in a safe and sound manner with level of activity reasonably related to the organization's business needs and capacity to fulfill obligations. 12 C.F.R. 225.142.

  - The board of directors, a duly authorized committee thereof or the internal auditors should review periodically (at least monthly) all financial contract positions to insure conformity with such policies and limits.

» Interagency Guidelines Establishing Information Security Standards (12 C.F.R. Part 225, Appendix F). *See* description in corresponding OCC regulations described above.

9. Resolution Plans (12 C.F.R. Part 243, applicable to bank holding companies with $50 billion or more in total assets)

» Resolution plans required under Section 165(d) of the Dodd-Frank Act for bank holding companies with $50 billion or more in total assets (12 C.F.R. 243.3(e)). *See* description in corresponding FDIC regulation at 12 C.F.R. 381.3(e) discussed above.

10. Proprietary Trading and Certain Interests in and Relationships with Covered Funds (12 C.F.R. Part 248, applicable to state member banks and bank holding companies)

» Volcker Rule (12 C.F.R. Part 248). *See* corresponding OCC regulations described above.

11. Regulation YY – Enhanced Prudential Standards (12 C.F.R. Part 252, applicable to certain bank holding companies, as noted below)

» Board risk committee requirements, applicable to publicly traded bank holding companies with total assets

of $10 billion or more, and bank holding companies (whether or not publicly traded) with total assets of $50 billion or more (12 C.F.R. 252.22; 252.33).

- A publicly traded bank holding company with total assets of $10 billion or more, and a bank holding company (whether or not publicly traded) with total assets of $50 billion or more, must maintain a risk committee of the board of directors that approves and periodically reviews the risk-management policies of the bank holding company's global operations and oversees the operation of its global risk-management framework.
    - *The risk committee must have a formal, written charter that is approved by the bank holding company's board of directors; it must meet at least quarterly, and otherwise as needed; and it must fully document and maintain records of its proceedings, including risk-management decisions.*
    - *The risk committee must have least one member having experience in identifying, assessing, and managing risk exposures of large, complex firms (if the bank holding company has $50 billion or more in assets, these must be large, complex financial firms); and it must be chaired by a director meeting the regulation's independence criteria.*
- A bank holding company with $50 billion or more in total assets (whether or not it is publicly traded) must also satisfy the following additional requirements:
    - *The risk committee must be an independent committee of the board of directors that has, as its sole and exclusive function, responsibility for the risk-management policies of the bank holding company's global operations and oversight of the operation of the bank holding company's global risk-management framework.*
    - *The risk committee must report directly to the bank holding company's board of directors.*
    - *The risk committee must receive and review regular reports on not less than a quarterly basis from the chief risk officer.*
    - *See the description of enhanced prudential standards immediately below for additional responsibilities with respect to liquidity risk management.*

» Additional enhanced prudential standards applicable to bank holding companies with $50 billion or more in total assets (12 C.F.R. Part 252, Subpart D).

- The board of directors must:
    - *approve the bank holding company's liquidity risk tolerance at least annually;*
    - *review at least semiannually information provided by senior management to determine whether the bank holding company is operating in accordance with its established liquidity risk tolerance; and*
    - *approve and periodically review the liquidity risk management strategies, policies, and procedures established by senior management.*
- The risk committee (or a designated subcommittee of such committee composed of members of the board of directors) must approve the contingency funding plan at least annually, and must approve any material revisions to the plan prior to their implementation.
- The board or risk committee must receive reports from senior management at least quarterly regarding the bank holding company's liquidity risk profile and liquidity risk tolerance.
    - *The board or risk committee also must receive reports from the independent review function of material liquidity risk management issues for corrective action, to the extent permitted by applicable law.*
- The risk committee must receive documentation of management's methodology for making cash flow pro-

jections and the included assumptions.

» Annual Company-Run Stress Tests, applicable to state member banks and bank holding companies with greater than $10 billion in total assets (12 C.F.R. Part 252, subparts B and F), and Annual Supervisory Stress Tests, applicable to bank holding companies with $50 billion or more in total assets (12 C.F.R. Part 252, Subpart E).

- With respect to the company-run stress tests, see description in corresponding OCC regulations discussed above.
- In addition, with respect to a bank holding company with greater than $50 billion in total assets, the board of directors and senior management specifically must consider the results of the annual company-run stress tests, as well as the supervisory stress tests, as appropriate:
  - *As part of the bank holding company's capital plan and capital planning process, including when making changes to the company's capital structure (including the level and composition of capital);*
  - *When assessing the bank holding company's exposures, concentrations, and risk positions; and*
  - *In the development or implementation of any plans of the bank holding company for recovery or resolution. 12 C.F.R. 252.47; 252.56(c)(3).*

II. Matters to be Addressed by Board of Directors Pursuant to Agency Guidance

A. OCC

1. The Director's Book: The Role of a National Bank Director

[*The following are selected excerpts from this 120-page guidance*]

The board sets the tone and direction of the bank and establishes guidelines on the nature and amount of risk the bank may take. The board oversees and supports management's efforts, reviews management's recommendations before approving or rejecting them, and makes sure that adequate controls and systems exist to identify and manage risks and address problems.

» The board establishes the bank's risk tolerance by approving policies that set standards for the nature and level of risk the bank is willing to assume. These policies should generally be written and periodically reviewed and updated.

» The board should ensure that bank management adequately identifies the risks associated with particular activities and has put in place systems and controls to manage those risks.

In difficult economic times or when management is ineffective, the board must evaluate the bank's problems, take appropriate corrective actions, and, when necessary, keep the bank operating until the board ensures that management is again effective and the bank's problems have been resolved.

A board should perform a self-assessment of its effectiveness periodically and determine whether it is taking the steps necessary to correct deficiencies. It also should review how well board committees are meeting their responsibilities.

After adopting policies, the board must ensure that its guidance is effectively communicated and adhered to throughout the bank (e.g., through a well-designed monitoring system).

The board must establish an appropriate corporate culture and set the "tone at the top," hire and retain competent management, stay informed about the bank's operating environment, and ensure that the bank has a risk management system suitable for the bank's size and activities. The board also must oversee the bank's business performance and serve community credit needs. Additional detail follows:

» **ESTABLISH AN APPROPRIATE CULTURE.** The board of directors must create a corporate culture and work environment that supports and encourages responsible, professional, and ethical behavior. The board is responsible for overseeing the development, periodic review, and monitoring of the code of ethics and other insider policies that address conduct, conflicts of interest, and other relevant issues.

» **HIRE AND RETAIN COMPETENT MANAGEMENT.** One of the board's most fundamental responsibilities is to select and retain competent management. When a bank hires a chief executive officer ("CEO"), the board or a designated board committee should actively manage the selection process.

- The board should review the performance of the CEO and other selected senior officers, as appropriate, and should consider requiring performance appraisals for all bank employees.

- The board should tailor the compensation package to the bank's size and financial condition, and the nature, scope, and complexities of its operations. The boards of

banks that use incentive compensation to a significant degree should actively oversee the development and operation of incentive compensation policies, systems, and related control processes.

- *The board should directly approve compensation programs involving senior executives, closely monitor payments relative to risk outcomes, and approve and document any material exceptions.*

- *Banks should establish a compensation committee that reports to the board to administer the organization's incentive compensation programs. Smaller banks with less complex incentive compensation programs may not find it necessary or appropriate to require specially tailored board expertise or to retain and use outside experts in this area.*

- The board or a designated committee should monitor personnel turnover rates to evaluate whether the bank is retaining the expertise and human resources needed to fulfill its goals. The board also should verify that the bank has adequate training programs to support needed skill levels and to keep personnel up-to-date on developments in the financial services industry.

- The board should develop a management succession policy to address the loss of the CEO and other key executives. The board should review these contingency plans annually to determine if they remain workable.

» **STAY INFORMED ABOUT THE BANK'S OPERATING ENVIRONMENT.** Directors should understand generally both the bank's business environment and the legal and regulatory framework within which the bank's activities operate.

- Some statutes and related regulations that merit special attention involve the following topics:

  - *Corporate governance (Sarbanes-Oxley; 12 C.F.R. 363)*

  - *Lending limits (12 U.S.C. 84; 12 C.F.R. 32)*

  - *Insider transactions (12 U.S.C. 375, 375a, 375b, 1972; 12 C.F.R. 31, 215)*

  - *Transactions with affiliates (12 U.S.C. 371c, 371c-1; 12 C.F.R. 223)*

  - *Safe and sound banking practices (12 C.F.R. 30)*

  - *Reporting requirements (12 U.S.C. 161)*

  - *Other laws and regulations (securities laws, antitrust laws, laws restricting management interlocks, anti-tying laws, criminal laws).*

- In addition, the bank's board must carefully review holding company policies that affect the bank to ensure that they adequately serve the bank. The board is responsible for either approving or recording its lack of approval of holding company directives that affect the bank and then monitoring those directives, notifying the holding company to discuss modifications, and considering further appropriate actions if necessary.

- The board of a holding company's subsidiary bank should be aware of the activities and condition of its holding company affiliates. In addition, the board at the bank level must oversee the bank's own subsidiaries and verify that effective controls are maintained. The bank's board should confirm that it has authority to audit operations and review findings of the subsidiary's own internal or external auditors.

» **MAINTAIN AN APPROPRIATE BOARD STRUCTURE.** The best committee structure for a bank depends on the bank's size, scope of operation, and risk profile, the board's composition, and individual directors' expertise. Committees discussed in the guidance include the executive committee, audit committee, loan committee, asset/liability management committee, risk management committee, fiduciary committee, compensation committee,

and corporate governance/nominating committee.

- Board committees typically oversee the bank's risk management by ensuring that management has implemented sound policies and procedures, either written or verbal; accurate and reliable risk measurement systems; timely and meaningful risk reporting processes; and effective risk controls, such as policy limits, authorizations, and product approvals. Some committees are required by regulation:
  - *An audit committee is required for any bank with assets in excess of $500 million and must be composed entirely of outside directors.*
  - *A trust audit committee is required for a bank with trust powers.*
  - *Audit, compensation, and corporate governance/nominating committees are required for banks whose securities are registered with the SEC or the OCC and must be composed entirely of independent directors.*

» **MONITOR OPERATIONS.** The board remains ultimately responsible for monitoring the bank's operations. The board can monitor the bank's operations through management reports, but it must do more than merely accept and review these reports; it must be confident that they are accurate, reliable, and contain sufficient details to allow effective monitoring.

- The board should ensure that management has incorporated a sound system of internal controls into the bank's daily operating procedures.
- A board may evaluate whether it is meeting its oversight responsibilities through a comprehensive audit and control program, as discussed in the guidance.
- The board should actively support the compliance function.

» **OVERSEE INFORMATION TECHNOLOGY ACTIVITIES.** The board must ensure that the information provided by management in IT reports is accurate, timely, and sufficiently detailed to oversee the bank's safe and sound operation. Board and management responsibilities include vendor management and safeguarding customers' nonpublic information.

- The board should actively demonstrate that it understands the bank's IT infrastructure, inherent risks, and existing controls. Both the chief technology officer and the information security officer should provide periodic updates on the bank's IT infrastructure and operations to the board.
- The board should review and approve adequate disaster recovery and business continuity plans every year.
- The board should also review and approve an adequate information security program annually, or as frequently as it is necessary to revise the program based on known vulnerabilities and threats.

» **CONSIDER A CONFIDENTIAL REPORTING SYSTEM.** Boards should consider the benefits of implementing several reporting platforms, such as discussions with supervisors, confidential conversations with human resources professionals, secure company Web sites and e-mail, and anonymous tip lines. The Sarbanes-Oxley Act requires public banking companies to implement a confidential system for reporting information regarding questionable accounting or auditing matters, known as the "whistleblower" provision. The existence of a confidential reporting system indicates that the board gives prompt attention to ethics lapses and other inappropriate or illegal activity. Having such a system emphasizes the responsibility that all employees have for leadership and ethical behavior—including reporting suspected wrongdoing.

» **OVERSEE BUSINESS PERFORMANCE.** A board should receive adequate financial data and analyses as detailed in the guidance. The board should identify the reports it wants to receive from management and their frequency. Key performance reports should enable the board to evaluate the amount of risk being taken, compliance

with the board's risk tolerances, and the adequacy of the bank's risk management processes.

- This section describes certain business performance measures, as well as key areas to monitor (asset quality, liquidity and interest rate risk positions, new products and services, noninterest earnings, off-balance-sheet items, and dividends). *See also* Detecting Red Flags in Board Reports – A Guide for Directors for more guidance on board reports.

- When evaluating the quality of earnings, directors should understand the soundness of the bank's operations and the interrelationships among operating statistics. Directors should ensure, for instance, that the bank does not artificially inflate earnings by delaying chargeoffs or inadequately providing for loan and lease losses.

» **SERVE COMMUNITY CREDIT NEEDS.** A board is responsible for ensuring that CRA efforts are an important element in a bank's plans and policies and that those efforts focus on performance rather than outreach, marketing, or other aims. A board should evaluate whether any areas of the bank's community have credit needs that are unmet and whether any changes to the bank's current plans or policies are appropriate.

» **STRATEGIC PLANNING.** The board should reassess the long-term strategic plan periodically to consider new opportunities or to respond to unanticipated external developments. The board should approve short-term business plans after concluding that they are realistic and compatible with the bank's tolerance for risk.

- The board should review and approve any proposed departures from the bank's strategic and business plans before they take place. For example, the board should have a planning, review, and approval process for major new activities or products that bank management proposes.

» **POLICIES.** The board or its designated committee should periodically review policies and oversee revisions as necessary to ensure that they remain consistent with the bank's goals and risk tolerance. The board should specify appropriate tools to measure and monitor the risks and should have a way to report risks to all responsible parties before the bank engages in a new activity. Major policy areas discussed in the guidance include:

» **LOAN PORTFOLIO MANAGEMENT.** The board should oversee loan portfolio management to control risks and maintain profitable lending operations. In addition to the general loan policy, the board should direct management to establish an internal loan review program that is independent of the lending function; the loan review function should report directly to the board or its audit committee.

- The board and management use the information drawn from loan portfolio reviews to assess whether the overall loan policy is effective, to maintain an adequate ALLL, and to serve as an early warning system for identifying underlying problems.

- The board must ensure that the bank has a program for developing, maintaining, and documenting a comprehensive, systematic, and consistently applied process for determining the amounts of the ALLL and the provision for loan and lease losses.

  - *The board is responsible for overseeing management's significant judgments and estimates pertaining to the determination of an appropriate ALLL.*

  - *Among other responsibilities, the board should review and approve the bank's ALLL policies and procedures at least annually, and review management's assessment and justification for the amounts estimated and reported each period for the ALLL and the provision for loan and lease losses.*

» **ASSET/LIABILITY MANAGEMENT.** The ALM policy should address the board's tolerances for interest rate and

liquidity risks and should establish procedures for measuring, monitoring, and controlling these risks.

- When considering asset/liability management activities, the board should scrutinize the following practices or conditions: excessive growth objectives; heavy dependence on volatile liabilities; exposure to a significant number of products with embedded options; gaps between asset and liability maturities or between rate-sensitive assets and liabilities at various maturity time frames; asset/liability expansion, both on- or off-balance sheet, without an accompanying increase in capital support; failure to diversify assets or funding sources; inadequate controls over securitized asset programs; and lack of expertise or control over off-balance-sheet derivative activities or other complex investment or risk management transactions.

» **INVESTMENT ACTIVITIES.** The board must ensure the bank's investment activities comply with applicable legal requirements. While the board may seek advice from technically competent managers or external sources, such as correspondent banks, brokerage houses, or consulting services, the board may not delegate its responsibility for overseeing the investment portfolio.

- The board should review the portfolio as necessary to confirm that the risk level remains acceptable and consistent with previously approved portfolio objectives.

- The board should direct management to establish systems with objectives and limits for each portfolio, taking into account applicable laws, regulations, and current accounting standards for each part of the portfolio.

- When considering investment activities, the board should scrutinize the following practices or conditions: failure to select securities dealers carefully; efforts to obtain higher yields without regard for other portfolio objectives; purchase of low-quality investments to obtain higher yields; purchase of structured securities without appropriate due diligence; failure to adequately diversify investments; failure to consider pledging requirements in investment decisions; failure to institute adequate internal controls for investment and trading activities; and failure to ensure the investment portfolio complies with current accounting standards.

» **FIDUCIARY ACTIVITIES.** Regardless of the scope of the fiduciary activities, the board is responsible for monitoring its administration. The board must protect the bank's fiduciary reputation, as well as the customer's assets, by having effective policies and procedures, management information systems, and risk management practices.

- The board should confirm that individuals who administer fiduciary activities at the bank are knowledgeable and competent, and have high personal integrity.

- The board should ascertain that internal controls and compliance management systems are adequate to minimize compliance, operational, reputation, and strategic risks associated with fiduciary activities.

- When considering fiduciary activities, the board should scrutinize the following practices or conditions: opening of new accounts not in compliance with account acceptance guidelines; purchasing of securities not previously approved by the board or investment committee; higher than anticipated yields on investment portfolios, collective investment funds, or advised mutual funds; existence of accounts with unusually high cash balances or large or extended overdrafts; failure to institute adequate internal controls for fiduciary activities; losses or settlements arising from actual or threatened litigation that are significant in either size or volume; and any situations that give rise to a conflict of interest.

» **INSIDER ACTIVITIES.** The board must adopt and enforce strong written insider policies governing the bank's relationship to insiders and their related interests. The board must adopt similar policies to cover bank officers and employees.

- The board must establish a method to administer and monitor compliance with the bank's insider policies. The board should require management to develop training and awareness programs covering insider issues and should establish lines of communication outside of the normal chain of command. The board should monitor questions and responses periodically to ensure consistent interpretations.

- In addition to other issues discussed elsewhere in the guidance, the following practices or conditions should trigger additional board scrutiny: transactions resulting in a conflict of interest; payment of excessive compensation or unjustified fees; fees paid to insiders for specific services should be based on cost, cost plus a reasonable profit, or current market value; and failure to comply with laws and regulations.

» Whether an administrative action is entered into by consent or imposed through an administrative proceeding, all directors are ultimately responsible for the bank's compliance with the action.

2. OCC Publication: Detecting Red Flags in Board Reports – A Guide for Directors (revised in 2004, reprinted in September 2013)

» The board can monitor the operations of the bank through management reports, but it must do more than merely accept and review these reports; it must be confident of their accuracy and reliability. Boards of directors should regularly receive reports on:

» **FINANCIAL PERFORMANCE** (including with respect to capital, asset quality, earnings, liquidity, market risk, and balance sheet growth).

- Financial reports should focus on comparative financial statements and key financial performance ratios and highlight areas of key risks. In reviewing these items, directors should identify any item that has changed significantly or that varies significantly from the budget, generally 10 percent or more, and should ask management to explain the deviation.

- Directors should regularly receive and review reports from management that contain key financial performance ratios and trends that facilitate effective monitoring of risk and financial performance. Directors should determine the reason for significant variances in the bank's performance when compared with the peer group.

- *Capital*. Directors should monitor the following ratios to help ensure compliance with regulatory minimum requirements: leverage ratio, tier 1 risk-based ratio and total risk-based ratio. Cash dividends/net income and equity growth rate versus asset growth rate ratios also may be useful.

- *Asset quality*. Directors should ensure the existence of adequate underwriting and risk selection standards, sound credit administration practices, and appropriate risk identification practices.

  - *Directors should consider the adequacy of ALLL; the level, distribution, severity, and trend of problem, classified, nonaccrual, restructured, delinquent, and nonperforming assets; the existence of concentrations of credit; credit risk arising from off-balance-sheet transactions; loan growth; and the volume and nature of credit policy and documentation exceptions.*

  - *In addition to reviewing reports prepared by management, directors should regularly review the following credit risk and asset quality leading indicators for signs of increasing credit risk: loan growth, loans to equity, change in portfolio mix, loans to assets, loan yield, noncurrent loans and leases/equity capital, ALLL/total loans and leases, ALL/net loans and leases, noncurrent loans and leases/ALLL, and net loan and lease losses/average loans and leases.*

- *Earnings*. The directors' review of earnings should focus

on the quantity, trend, and sustainability or quality of earnings. The level and trend of the following measures are important in evaluating earnings: net income/average assets, net income/average total equity, net interest income/average earning assets, noninterest income/average assets, overhead (noninterest) expense/average assets, and provision expense/average assets.

- *Liquidity*. Directors should compare the bank's current level of liquidity, plus liquidity that would likely be available from other sources, with its funding needs to determine whether the bank's funds management practices are adequate.

- *Market risk*. To assess the bank's market risk, directors should determine how changes in interest rates, foreign exchange rates, commodity prices, or equity prices could reduce the bank's earnings or capital.

- *Balance sheet growth*. Directors should look at the effect of growth on the bank's exposure to risk in key categories, such as asset quality, earnings, capital, and liquidity. Directors should identify growth patterns by comparing historical and budgeted growth rates for assets, capital, loans, volatile liabilities, core deposits, and income and expenses. Comparing the bank's growth rates with those of its peers may also indicate whether the bank is growing inordinately.

» **CREDIT RISK MANAGEMENT** (including with respect to credit quality, ALLL, and a summary of new credits approved, loans renewed, concentrations of credit, and participations purchased and sold).

- Directors should understand the portfolio's industry and geographic concentrations, average risk ratings, and other credit risk characteristics. They should also ensure that the bank has appropriate staffing and expertise for all of its lending activities and that management is capable of effectively managing the risks being assumed.

- Directors should monitor adverse trends in the loan portfolio and should judge the adequacy of the ALLL by reviewing the loan reports. The board, or a loan committee of directors, should receive information on new and renewed loans that represent large single-borrower exposures, material participations purchased and sold, past-due and nonperforming loans, other real estate owned ("OREO"), problem loans and trends in risk ratings identified by management and examiners, charge-offs and recoveries, management's analyses of the adequacy of the ALLL, composition of the loan portfolio, concentrations of credit, credit and collateral exceptions, and customers with large total borrowings.

- *Credit quality.* Directors review the following reports to assess loan quality: risk rating reports, problem loan reports, rating migration reports, past-due and nonaccrual reports, renegotiated and restructured loan reports, OREO reports, exception reports, and concentration reports.

- *ALLL*. Directors should review the following information to determine whether the ALLL is adequate: management's quarterly evaluation of the adequacy of the ALLL prepared as of call report dates; management's problem loan list; charge-off and recovery experience; a reconcilement of the ALLL for the current period and previous year-end; and any independent analysis of the ALLL (e.g., external loan review).

» **LIQUIDITY RISK MANAGEMENT.** The board and senior management are responsible for understanding the nature and level of liquidity risk assumed by the bank and the tools used to manage that risk. The board and senior management should also ensure that the bank's funding strategy and its implementation are consistent with their expressed risk tolerance.

- The board of directors' primary duties in this area should include establishing and guiding the bank's strategic direction and tolerance for liquidity risk; selecting senior managers who will have the authority

and responsibility to manage liquidity risk; monitoring the bank's performance and overall liquidity risk profile; and ensuring that liquidity risk is identified, measured, monitored, and controlled.

- Directors should review regularly a complement of measurement tools, including forward-looking risk measures. The following reports should assist directors in assessing the bank's liquidity risk: liquidity risk report, funds provider report, projected needs and sources, funds availability report, cash flow or funding gap report, funding concentration report, and the contingency funding plan.

- The following ratios can also be useful as liquidity risk indicators: loan to deposit ratio, net non-core funding dependence, net short-term liabilities/total assets, on-hand liquidity/total liabilities, and reliance on wholesale funding.

» **INTEREST RATE RISK MANAGEMENT.** The directors establish the bank's tolerance for interest rate risk and monitor its performance and overall interest rate risk profile. The directors also ensure that the level of interest rate risk is maintained at prudent levels and is supported by adequate capital.

- The board should request and review reports that measure the bank's current interest rate risk position relative to earnings at risk and capital at risk limits. The board should request and review gap reports, simulation models, and economic value sensitivity models.

- The following ratios can be useful as interest rate risk indicators: long-term assets/total assets, nonmaturity deposits/long-term assets, residential real estate/total assets, asset depreciation/tier 1 capital.

- The following management reports should assist directors in assessing the bank's interest rate risk: risk summary, earnings at risk, audit reports, capital at risk, and net interest margin analysis.

» **INVESTMENT PORTFOLIO MANAGEMENT** (including with respect to the selection of securities dealers; accounting classification of securities as held-to-maturity, available-for-sale, or trading; and investment reports to assess the overall quality, liquidity, and performance of the investment portfolio).

- Directors establish strategic direction and risk tolerance limits, review portfolio activity, assess risk profile, evaluate performance, and monitor management's compliance with authorized risk limits.

- *Selection of securities dealers*. Directors review and approve a list of securities firms with whom the bank is authorized to do business. Directors also provide management guidance on credit quality and other standards appropriate to ensure that dealers used by the bank are financially stable, reputable, and knowledgeable. The board of directors may want to consider prohibiting employees who purchase and sell securities for the bank from engaging in personal securities transactions with the same securities firms the bank uses for its transactions.

- *Categorization of securities*. Directors are ultimately responsible for effective oversight of a national bank's investment portfolio. However, a bank's board may delegate investment decision-making authority for all or a portion of its investment securities portfolio either to a nonaffiliated firm or to a person who is not an employee of the institution or one of its affiliates.

- *Investment reports*. Directors may find the following reports helpful in assessing the overall quality, liquidity, and performance of the investment portfolio: maturity breakdown, average maturity, and interest rate risk; distribution of credit ratings; adjusted historical cost for each security sector relative to its current market value; purchases and sales; and sensitivity analysis of the value of the portfolio in different interest rate environments.

» Financial derivatives and off-balance-sheet activities (including with respect to financial derivatives, asset securi-

tizations, credit commitments, and mortgage banking).

- The board is responsible for communicating its risk tolerance limits to management, making sure that management establishes control mechanisms that reflect that risk tolerance, reviewing risk reports, confirming compliance with policy limits, and determining that the bank uses these products for approved purposes. Directors must make sure that the bank has appropriate expertise to identify, measure, monitor and control the entire risk spectrum of all products used.

- *Financial derivatives*. Directors should use the following types of reports to assess financial derivatives activity: credit risk exposures; trends in derivatives usage; compliance with policies and risk limits; results of stress testing; impact on income from derivatives.

- *Asset securitization*. The board must determine whether the bank has the necessary resources and expertise to engage effectively in this business. An effective board ensures that transactions are consistently and thoroughly supervised and monitored over the duration of the bank's involvement in these activities. Management reports to the board should include the performance of the underlying asset pools for all outstanding deals.

- The board of directors and bank management should ensure that:

    - *Independent risk management processes are in place to monitor securitization pool performance on an aggregate and individual transaction level.*

    - *Management uses conservative valuation assumptions and modeling methodologies to establish, evaluate, and adjust the carrying value of retained interests on a regular and timely basis.*

    - *Audit or internal review staffs periodically review data integrity, model algorithms, key underlying assumptions, and the appropriateness of the valuation and modeling process for the securitized assets retained by the institution. The findings of such reviews should be reported directly to the board or an appropriate board committee.*

    - *Management maintains accurate and timely risk-based capital calculations, including recognition and reporting of any recourse obligation resulting from securitization activity.*

    - *Internal limits are in place to govern the maximum amount of retained interests as a percentage of total equity capital.*

    - *The institution has a realistic liquidity plan in place in case of market disruptions.*

    - *Transactions do not create recourse to the bank.*

    - *Reports that the board receives in respect of revolving transactions (credit cards, home equity lines, etc.) and installment loans, as appropriate, include: the gross and net portfolio yield; delinquencies; the charge-off rate; the base rate (investor coupon plus servicing fees); monthly excess spread; the rolling three-month average excess spread; the monthly payment rate; principal prepayment speeds; outstanding principal compared with original security size; residuals; policy exceptions; covenant compliance; exposure limits by type of transaction; and aggregate transactions outstanding.*

- *Credit commitments*. The board should ensure that bank policy supports a loan officer's refusal to advance funds when a borrower is financially troubled, covenants have been broken, or other adverse conditions have arisen. The board should receive reports from management projecting the funding sources for loan commitments and lines of credits (based on the anticipated usage of such commitments and lines).

- *Mortgage banking*. The board should ensure that prudent risk management practices and controls are in place for its mortgage banking activities.

- *The board of directors should ensure that the following key systems and controls are in place: comprehensive documentation standards for all aspects of mortgage banking; MSA impairment analyses that use reasonable and supportable assumptions; systems to measure and control interest rate risk; accurate financial reporting systems, controls, and limits; timely and accurate tracking of quality control exceptions; appropriate tracking and collecting of required mortgage loan documents; appropriate monitoring and managing of risks associated with third-party originated loans; and adequate internal audit coverage.*

- *The board should receive reports on: internal audit, quality control, and compliance findings; policy exceptions; valuation of MSAs; hedged and un-hedged positions; mark-to-market analyses; profitability; monthly production volume; loan inventory aging; delinquencies and foreclosures; status of reserves; and operational efficiency.*

» **AUDITS AND INTERNAL CONTROL.**

- Directors cannot delegate their responsibility for oversight of the auditing function. However, they may delegate the design, implementation, and monitoring of specific internal controls to management and the testing and assessment of internal controls to others.

- The board of directors should consider whether the bank's control systems and auditing methods, records, and procedures are proper in relation to the bank's: size; organization and ownership characteristics; business activities and product lines; operational diversity and complexity; risk profile; methods of processing data; and applicable legal and regulatory requirements.

- The board of directors, or its audit committee, should meet regularly (at least quarterly) with the bank's internal auditor and review information on matters pertaining to the effectiveness of control systems and risk management processes and progress toward achieving the bank's overall audit objectives. Executive summary reports, or audit information packages, should be a part of these reviews and should include:

  - *Status reports on meeting the annual audit plan or schedule, including any adjustments to the plan or schedule, and activity reports on audits completed, in process, and deferred or cancelled.*

  - *Information about audit staffing, independence, and training.*

  - *Discussion of significant accounting issues or regulatory issuances pertaining to audit or controls.*

  - *Copies of individual audit reports issued during the quarter or summaries of audits conducted and significant issues noted.*

  - *Summaries of information technology, fiduciary, and consumer compliance audits, as warranted.*

  - *Risk assessments performed or summaries thereof.*

  - *Significant outstanding audit and control issues, in the form of tracking reports that describe the issues, when the issues were discovered, the person responsible for corrective action, the promised date of correction, and status of corrective action.*

» **CONSUMER COMPLIANCE** (including with respect to fair lending, the CRA, and BSA/AML).

- To effectively monitor compliance with consumer laws and regulations, the board must receive timely and accurate reports on compliance matters. The complexity and extent of reporting will vary with the complexity and extent of the bank's operations, products, services, customers, and geographies served. The designated compliance officer should have direct access to the board.

- Although compliance with all consumer laws and regulations should be important to all boards of directors, the *Detecting Red Flags* guide states that boards often

place special emphasis on fair lending, the Community Reinvestment Act (CRA), and the Bank Secrecy Act (BSA).

- *CRA*. While the regulation no longer requires directors to document how actively they participate in community groups or civic organizations, the entire board's attention, leadership, and commitment are essential to successful CRA performance. Although the bank is not required to assess its CRA progress, periodic self-assessments can help the board determine the bank's progress toward achieving its internal CRA goals and performance objectives.

- *BSA/AML*. The board should ensure that the bank's program for BSA compliance includes proper internal controls, independent testing, appropriate staff training, and updates whenever regulatory changes take place.

  - *Specifically, directors should ensure that the BSA compliance program includes appropriate account opening and customer identification verification procedures, determine the nature and purpose of the account, and identify the bank's services or products the customer will use.*

  - *Additionally the BSA program should include monitoring systems and procedures to ensure that the bank is aware of any suspicious activities. Directors and bank management must be particularly alert to certain potentially high-risk accounts, services, and geographic areas described in the guidance.*

» **ASSET MANAGEMENT.**

- Although the board may assign functions related to the exercise of fiduciary powers to any director, officer, or employee of the bank, the board is ultimately responsible for any financial loss or reduction in shareholder value suffered by the bank.

- An effective board of directors will oversee the development of asset management-related risk limits, approve new products or services, and monitor on-going business plans. Boards of directors should expect to see routinely financial performance reports related to each asset management business.

- Directors generally find the following reports helpful in assessing the risks and financial performance of asset management activities: new business/lost business reports; investment reports; investment performance analyses; litigation reports; profitability/budget reports; trust bank capital and liquidity analysis reports; and fiduciary audit reports.

» **MANAGEMENT INFORMATION SYSTEMS.**

- The board should ensure that the bank has an adequate business continuity plan. The board should also ensure that the bank has appropriate policies, procedures, and controls in place to ensure that data systems have adequate safeguards to protect sensitive financial data and customer information and that key systems can be restored or accessed in the event of an emergency or a disaster.

- To assess a bank's information systems, the board must consider whether the MIS process provides the information necessary to manage the organization effectively. If vendors play important roles in the bank's information system, the board must ensure that the vendor's services and reports meet the same standards as those generated within the bank.

» **INTERNET BANKING.**

- The board should ensure that management possesses the knowledge and skills to manage the bank's use of Internet banking technology and technology-related risks.

- In describing the board's role, the *Detecting Red Flags* guide states that the board reviews, approves, and monitors Internet banking technology-related projects. They determine whether the technology and products are in line with the bank's strategic goals and meet a need in their market. The board receives regular reports on the

technologies employed, the risks assumed, and how those risks are managed.

» **OCC'S OVERALL ASSESSMENT** (including with respect to ratings and the risk assessment system).

- The board should pay particular attention to weaknesses and adverse trends identified during the examination and to the actions management plans to take or have already taken to address those weaknesses.

3. OCC Bulletins, Circulars and Advisory Letters

a. OCC 2015-36 – Tax Refund-Related Products (8/4/2015)

» If the bank offers any tax refund-related product, the bank's board of directors should require the bank to maintain sound risk management policies, procedures, and practices to oversee all such products, particularly those involving third-party tax preparers.

- This oversight should include a board role in a comprehensive due diligence process for any new products and material changes to existing products, as detailed in other guidance.

- The board should also require the bank's compliance management program to identify, measure, monitor, and control the consumer protection risks associated with higher fees, compensation incentives, and reliance by customers on third-party tax preparers for guidance.

» Management should ensure compliance with bank policies and applicable laws and regulations through periodic reviews that are regularly reported to the board of directors.

- The results of the bank's reviews of third-party tax preparers who offer tax refund-related products on the bank's behalf are typically documented, shared with the board of directors, and available to examiners.

- The guidance also describes various other reports and analysis customarily reported to the board, including with respect to production and portfolio trends, exception tracking, delinquency and loss distribution trends by product and originator channel, and a number of other items.

b. OCC 2014-52 – Matters Requiring Attention (10/30/2014)

» MRAs, among other things, are the means by which supervisory concerns are communicated in writing to bank boards and management teams.

» When concerns are included in a formal written communication to the bank:

- The board may be required as part of the corrective action to determine the root cause in situations when the root cause is not immediately evident.

- Inaction could lead to violations of law in certain instances or additional supervisory actions, including enforcement actions or civil money penalties for the bank, the bank's board of directors, or management.

- The board and management must ensure that the corrective action is timely, measurable, and sustainable.

- If management is unable to provide an action plan during the examination, it must submit to the OCC a board-approved plan within 30 days of receipt of the formal written communication.

» The OCC expects the bank's board of directors to ensure timely and effective correction of the practices described in an MRA. Those expectations include:

- holding management accountable for the deficient practices;

- directing management to develop and implement corrective actions;
- approving the necessary changes to the bank's policies, processes, procedures, and controls; and
- establishing processes to monitor progress and verify and validate the effectiveness of management's corrective actions.

c. OCC 2013-33 – Use and Review of Independent Consultants in Enforcement Actions: Guidance for Bankers (11/12/2013)

» The use of an independent consultant does not absolve bank management or a bank's board of directors of their responsibility for ensuring that all needed corrective actions are identified and implemented.

» The bank should ensure the proposed engagement contract it submits for a determination of supervisory no objection guarantees, among other things, that the board of directors receives a final report.

» Once the independent consultant's final written report and findings have been presented to the bank's board and reviewed by the OCC, the bank should prepare a plan to address the findings of the independent consultant and to implement the board's responses. Such plans should be approved by the bank's board of directors and are subject to OCC review and a written determination of supervisory no objection before they can be implemented.

d. OCC 2013-29 – Third Party Relationships (10/30/2013)

» A bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws.

» Responsibilities of the board of directors include the following:

- Ensure an effective process is in place to manage risks related to third-party relationships in a manner consistent with the bank's strategic goals, organizational objectives, and risk appetite.
- Approve the bank's risk-based policies that govern the third-party risk management process and identify critical activities.
- Review and approve management plans for using third parties that involve critical activities.
- Review summary of due diligence results and management's recommendations to use third parties that involve critical activities.
- Approve contracts with third parties that involve critical activities.
- Review the results of management's ongoing monitoring of third-party relationships involving critical activities.
- Ensure management takes appropriate actions to remedy significant deterioration in performance or address changing risks or material issues identified through ongoing monitoring.
- Review results of periodic independent reviews of the bank's third-party risk management process.

» "Critical activities" are defined in the guidance as significant bank functions (e.g., payments, clearing, settlements, custody) or significant shared services (e.g., information technology), or other activities that:

- could cause a bank to face significant risk if the third

party fails to meet expectations.

- could have significant customer impacts.
- require significant investment in resources to implement the third-party relationship and manage the risk.
- could have a major impact on bank operations if the bank has to find an alternate third party or if the outsourced activity has to be brought in-house.

e. OCC 2013-15 – Bank Appeals Process: Guidance for Bankers (6/7/2013)

» A formal appeal represents written communication to a Deputy Comptroller or the Ombudsman expressing disagreement with the final supervisory conclusions. A formal appeal must have board approval.

f. OCC 2013-14 – CFTC Swap Clearing Rules: Mandatory Clearing of Certain Interest Rate and Credit Default Swaps (6/6/2013)

» A bank wishing to utilize an exception from the CFTC's mandatory swap clearing rules should carefully review the CFTC's rules and guidance to ensure it qualifies for the exception. Among other things, if a bank is a public company or a subsidiary of a public company, the appropriate committee of the bank's board of directors may have to review and approve the bank's decision to use a clearing exception.

g. OCC 2013-40 – Guidance on Supervisory Concerns and Expectations Regarding Deposit Advance Products (11/20/2013)

» Bank policies regarding the underwriting of deposit advance loan products should be in writing and approved by the bank's board of directors, and be consistent with the bank's general underwriting standards and risk appetite. The guidance describes a number of factors that the bank should address in its written underwriting policies for these products.

» Examiners will assess bank management's ability to administer a deposit advance program and board oversight of the program.

» Results of management's oversight activities—including identified weaknesses that, should be documented and promptly addressed—should be reported periodically to the bank's board of directors or designated committee.

h. OCC 2012-16 – Capital Planning: Guidance for Evaluating Capital Planning and Adequacy (78 FR 70624, 6/7/2012)

» Capital planning assists the bank's board of directors and senior management to

- identify risks, improve their understanding of the bank's overall risks, set risk tolerance levels, and assess strategic choices in longer-term planning.
- identify vulnerabilities such as concentrations and assess their impact on capital.
- integrate business strategy, risk management, capital and liquidity planning decisions, including due diligence for a merger or acquisition.
- have a forward-looking assessment of the bank's capital needs, including capital needs that may arise from rapid changes in the economic and financial environment.

» A bank's success depends on the strong and independent oversight by its board of directors in all areas, including capital planning.

- The board should articulate to management its risk-tol-

erance level, for example by setting approved limits.

- The board should review the capital planning process and capital goals at least annually to ensure that a sufficient level of capital exists at all times to fully support the bank's overall risks and anticipated needs. When management provides the board with regular reports and updates, the board can clearly understand the financial resiliency of the bank.

- Through discussions with senior management, the board or its designee should evaluate both internal and external sources of capital in defining a strategy to build capital when necessary.

- Effective boards hold management accountable for identifying and taking corrective actions if shortcomings or weaknesses in the capital planning process become apparent or if the level of capital falls below identified needs.

- It is particularly important for a bank's board of directors to ensure the dividend level is prudent relative to the bank's financial position.

i. OCC 2011-27 – Prepaid Access Programs (7/6/2011)

» National banks that offer prepaid access devices to consumers should have a comprehensive risk management program ("prepaid access program") to identify, measure, monitor and control the risks related to these products. The board of directors should ensure it understands how the prepaid access program is expected to operate, the level and nature of risks it will bring to the bank, and its projected costs and revenues. "Prepaid access" refers to a wide range of devices that facilitate consumers' access to money electronically, including general purpose reloadable cards, payroll cards, government benefit cards, retail gift cards, mobile phones, and Internet sites.

» In consultation with bank management, the board should establish risk limits for the prepaid access program and outline expectations for compliance and performance reporting.

» In setting risk limits and other prepaid access program guidelines, the board of directors or its designee should:

- consult with relevant functional areas within the bank to gather data sufficient to understand the program's requirements, such as the need for expertise, staffing, and infrastructure, and the costs associated with these requirements. Relevant functional areas would include, for example, operations, information technology, audit, compliance and legal.

- identify specific program objectives, such as expected growth rates and size of the program in relation to the bank's total assets or capital.

- outline performance criteria, such as qualitative and quantitative benchmarks to evaluate success of the product; variance analyses (actual results versus projections) to detect and address adverse trends in a timely manner; and specific thresholds that, if met, would result in management taking action to change or discontinue the program.

- require periodic review of the program by the board of directors to determine whether changes in product capabilities, regulatory requirements, competitive factors, or other aspects of the business model result in changes to the bank's risk/reward analysis for the program.

j. OCC 2011-12 – Supervisory Guidance on Model Risk Management (4/4/2011)

» A bank's board and senior management should establish a strong model risk management framework that fits into the broader risk management of the organization.

- While the board is ultimately responsible, it generally delegates to senior management the responsibility for executing and maintaining an effective model risk management framework.
- In the same manner as for other major areas of risk, senior management, directly and through relevant committees, is responsible for regularly reporting to the board on significant model risk, from individual models and in the aggregate, and on compliance with policy.
- Board members should ensure that the level of model risk is within their tolerance and direct changes where appropriate.
- The board or its delegates should approve model risk management policies and review them annually to ensure consistent and rigorous practices across the organization.
- Findings from internal audit related to models should be documented and reported to the board or its appropriately delegated agent.

k. OCC 2011-11 – Risk Management Elements: Collective Investment Funds and Outsourced Arrangements (3/29/2011)

» A national bank's board of directors must ensure that a third party performs its functions in a safe and sound manner and in compliance with applicable laws and policy guidance.

» When considering whether to enter into a third-party relationship with a registered investment adviser ("RIA") or other vendor, the board and management should clearly identify the nature and scope of the relationship, given the bank's overall business strategy and objectives, and should ensure that third-party activities are clearly integrated with corporate strategic goals.

» The bank's board and management must first ensure that the RIA has systems in place to ensure that only eligible accounts will have access to the bank's collective investment funds.

» The decision to delegate specified responsibilities for a collective investment fund to a third-party vendor is a matter of fiduciary judgment. It requires a determination by a bank's board, or designee, that the delegation is prudent.

l. OCC 2008-5 – Risk Management Guidance – Divestiture of Certain Asset Management Businesses (3/6/2008)

» The OCC expects bank boards and management, when divesting bank-affiliated funds and associated advisers where ERISA accounts are involved, to ensure that all issues under ERISA are identified.

m. OCC 2007-21 – Supervision of National Trust Banks (6/26/2007)

» It is the responsibility of a national trust bank's management and board to implement a system to analyze and maintain adequate liquidity and capital.

- It is the responsibility of the board of directors and management of a national trust bank to ensure that capital and liquidity levels are adequate and that appropriate capital and liquidity planning processes are in place.

» Board-approved capital and liquidity policies should outline the board's philosophy and articulate responsibilities and expectations for the management of capital and liquidity.

» The board should regularly assess management's adherence to established policies and evaluate capital adequacy and overall levels and trends in liquidity.

n. OCC 2006-39 – Automated Clearing House Activities (9/1/2006)

» Both the board of directors and management are responsible for ensuring that the automated clearing house ("ACH") program does not expose the bank to excessive risk.

» The board's role is to establish the bank's overall business strategy and risk limits for the ACH program and to oversee management's implementation of the program.

» Adequate ACH policies and procedures generally include, among other things, board-approved risk tolerances that outline the types of activities the bank may conduct and the types of businesses approved for ACH transactions.

» The board should ensure that there is sufficient expertise to carry out the bank's ACH audit activities, whether the function is performed by internal audit staff or an external audit firm. The board should also ensure that auditors attend training periodically to ensure that their skills keep pace with any expansion in the bank's ACH program.

» Before a bank engages in high-risk ACH activities, the board of directors should consider carefully the risks associated with these activities, particularly the increased reputation, compliance, transaction, and credit risks. The board should provide clear direction to management on whether, or to what extent, the bank may engage in such ACH activities.

o. OCC 2004-20 – Risk Management of New, Expanded, or Modified Bank Products and Services (5/10/2004)

» Before deciding to introduce a significant new, expanded, or modified product or service to bank customers, management and the board should conduct due diligence to ensure they have a realistic understanding of the risks and rewards of the product or service being considered. Management and the board should clearly understand the rationale for offering the product or service.

» Although the board may delegate performance of managerial duties to others, it has the ultimate responsibility for ensuring that the bank is run in a safe and sound manner.

» In fulfilling its responsibilities, the board or its designee must ensure that a new, expanded, or modified bank product or service is consistent with the bank's strategic goals.

» Once the bank decides to introduce a new, expanded, or modified product or service and develops a business plan, the board and management should develop and implement adequate risk management processes to effectively control the risks of the activity. This should include:

- Expanding and amending bank policies and procedures, as appropriate, to ensure that they adequately address the product or service. Policies and procedures should establish accountability and provide for exception monitoring.
- Developing and implementing the information and reporting systems ("MIS") necessary to monitor adherence to established objectives and to properly supervise the product or service. MIS reports should contain key indicators to allow the board and management to effectively identify, measure, monitor, and control risk.
- Incorporating the product or service into the bank's audit and compliance processes to ensure adherence with bank policies and procedures and customer safeguards.

» Management and the board should have appropriate performance and monitoring systems in place to allow them to assess whether the product or service is

meeting operational and strategic expectations. Such systems should:

- Include limits on the size of acceptable risk exposure that management and the board are willing to assume.
- Identify specific objectives and performance criteria to evaluate success of the product or service. The performance criteria should include quantitative benchmarks that will serve as a means to evaluate success of the product or service.
- Reflect a process that periodically compares actual results with projections and qualitative benchmarks, to detect and address adverse trends or concerns in a timely manner.
- Trigger changes in the business plan, when appropriate, based on the performance of the product or service. Such changes may include exiting the activity should actual results fail to achieve projections.

p. AL 2003-10 – Risk Management of Wireless Networks (12/9/2003)

» It is important that the board and management update the bank's security program before activating new systems, such as wireless networks, since the use of new technologies may render an existing security program ineffective.

» Wireless network solutions provide national banks with an alternative for systems development that requires effective board and management oversight.

q. OCC 2002-19 – Unsafe and Unsound Investment Portfolio Practices (5/22/2002)

» The board should review the bank's risk management framework for investment risks and confirm that it provides appropriate controls over the current level of risk.

» The board should also formally approve changes to policies and practices that permit increased risk tolerance.

r. OCC 2002-16 – Bank Use of Foreign-Based Third-Party Service Providers (5/15/2002)

» As with domestic outsourcing arrangements, the board of directors and senior management are responsible for understanding the risks associated with the bank's outsourcing relationships with foreign-based service providers and ensuring that effective risk management practices are in place.

s. AL 2000-10 – Payday Lending (11/27/2000)

» A bank's board of directors should be provided periodic reports, including compliance reports and audit reports, on the bank's payday lending activities.

t. OCC 2000-14 – Infrastructure Threats – Intrusion Risks (5/15/2000)

» Senior management and the board of directors are responsible for overseeing the development and implementation of their bank's security strategy and plan.

- Key elements to be included in those strategies and plans are an intrusion risk assessment plan (with respect to intrusions into bank computer systems), risk mitigation controls, intrusion response policies and procedures, and testing processes.

u. OCC Bulletin 99-15 – Subprime Lending: Risks and Rewards (4/5/1999)

» Before a bank engages in subprime lending, the board of

directors must have done comprehensive due diligence. Management and the board must fully understand the business and the inherent risks if they expect to mitigate them effectively, and they should conduct a realistic analysis of the competitive environment.

- It is critical that underwriting policies and procedures incorporate the risk tolerances established by the board and management.

- Quality control reports should be distributed to the board and senior management. The board and management should also ensure audit staffing and coverage adequate to render an opinion on the quality of the subprime unit's operations, including internal and accounting controls, compliance with laws and regulations, and adherence to accounting standards.

» *See also* Interagency Guidance on Subprime Lending described below.

v. OCC Bulletin 98-3 – Technology Risk Management: Guidance for Bankers and Examiners (2/4/1998)

» The OCC will evaluate whether senior management and the board of directors are sufficiently engaged in the planning process to manage the bank's technology-related risks. The board of directors and senior management should review, approve, and monitor technology projects that may have a significant impact on the bank's operations, earnings or capital. The board should be fully informed by senior management, on an ongoing basis, of the risks that technology projects may pose to the bank.

w. OCC-97-22 – Fiduciary Activities of National Banks (5/15/1997)

» Collective investment fund plan amendments should be approved by the bank's board of directors or its designee. A bank may delegate collective investment fund responsibilities to an investment advisor if the delegation is prudent; however, the board of directors, or its designee, should approve the delegation and ensure an agreement setting forth duties and responsibilities is in place.

x. AL 96-7 – Credit Card Preapproved Solicitations (9/25/1996)

» At a minimum, a risk management program for a preapproved credit card solicitation program should include, among other things, the reporting of appropriate risk management information to senior management and the board of directors. As appropriate, management should require the marketing staff to report appropriate market testing information to senior management and the board of directors.

y. OCC 96-25 – Fiduciary Risk Management of Derivatives and Mortgage-Backed Securities: Guidance for Bankers (4/30/1996)

» Fiduciary investment activities should be prudently conducted within the fiduciary risk management framework established by the board of directors. National banks should establish a reporting mechanism that ensures the board of directors is adequately informed concerning the nature and level(s) of investment risk taken in fiduciary accounts.

z. BB-93-54 – Questions and Answers Regarding Documentation Policy (11/2/1993)

» If a bank chooses to participate in the minimal loan documentation program for small business and farm loans (as explained in the Interagency Policy Statement on Documentation for Loans to Small- and Medium-sized Businesses and Farms, dated March 30, 1993), the board

should acknowledge the bank's participation in its meeting minutes and assign responsibility for maintaining sufficient records to comply with the program.

- This program generally permits well- or adequately-capitalized institutions with a satisfactory supervisory rating to identify a portion of their portfolio of small- and medium-sized business and farm loans that will be evaluated solely on performance and will be exempt from examiner criticism of documentation.

aa. EC-245 – Highly Leveraged Transactions (12/14/1988)

» The OCC expects boards of directors and management of national banks to ensure that their involvement in highly leveraged transactions is governed by sound policies, careful credit and legal analyses, appropriate controls, and sound management information systems. Examiners should determine whether a bank's board has adopted a written policy statement that clearly defines a highly leveraged transaction ("HLT"), as well as the bank's overall philosophy and objectives in financing HLTs.

- Among other things, the policy statement should include in-house limits on exposure for individual credits, specific industries, and the aggregate portfolio, to be reviewed at least annually by the board.

- Examiners should separately determine whether the board has approved a separate policy (that meets criteria specified in the guidance) for approving and reporting on HLTs to supplement policies used in the normal credit process.

    - *In addition, examiners should determine whether the board of directors and management have established policies on HLTs to minimize risks posed by potential legal and conflict-of-interest issues.*

- Examiners should determine whether a separate, specific MIS and analysis process is sufficiently detailed (under criteria specified in the guidance) to provide management and the board with periodic information on the overall size, quality and performance of the HLT portfolio.

bb. BC-216 – Securities Denominated in Foreign Currencies (9/11/1986)

» If a national bank chooses to hold foreign currency denominated investment securities, the board of directors or a board committee should approve and enforce policies to control foreign currency risks.

- These policies, at a minimum, should address: currency limits; gross and net open position limits; asset and liability mismatch (gap) limits; stop loss limits; individual purchase and sale authority limits; evaluation and periodic reevaluation of currency risk exposure, and country risk exposure; procedures for periodic revaluation; financial reporting considerations; appropriate management information systems and board or board committee information systems; and internal audit procedures.

cc. BC-58(Rev), Sup. 1 – Sale of Commemorative Coins (12/28/1983)

» Prudence and care should be exercised by boards of directors in formulating policies and procedures when purchasing commemorative coins. Dollar limits on coin inventories should be consistent with safe and sound banking practices.

» *See also* OCC Interp. Ltr. #840 (9/21/1998) ("To minimize the risk of [purchasing and selling commemorative coins issued by an entity other than the U.S. Mint], it is especially important that the board of directors establish policies and procedures which set dollar limits on coin inventories consistent with safe and sound banking practices.")

dd. BC-58(Rev) – Coin and Bullion (11/3/1981)

» The risks associated with coin and bullion activities should be fully evaluated by a bank's board of directors. Before a national bank commences such activities the board of directors should formally authorize the program and establish policies and procedures governing the activity. Those policies and procedures should include (among other things) position limits, reporting requirements to management and the establishment of accounting, internal control and audit systems for these operations.

4. Comptroller's Handbook

The Comptroller's Handbook is a collection of booklets that contain the concepts and procedures established by the OCC for the examination of national banks. The Foreword to the Handbook states that "OCC examiners consider the risks posed by and the materiality of the areas under examination to decide the scope and additional procedures to be followed. Examiners tailor the examinations to fit the operations of specific banks while fulfilling OCC and statutory requirements."

a. Asset Management

» The board of directors and senior management must be committed to risk management for processes to be effective. Acknowledged acceptance and oversight of the risk management process by the board and senior management is important. Institutions that have been successful in prudent risk taking have a corporate culture that balances risk controls and business initiatives. Directors must recognize their responsibility to provide proper oversight of asset management activities, and the official records of the board should clearly reflect the proper discharge of that responsibility.

» Directors must understand the asset management business, how asset management activities affect the bank's position and reputation, the bank's regulatory environment, and other external market factors. The board must recognize and understand existing risks and risks that may arise from new business initiatives, including risks that originate in bank and nonbank subsidiaries and affiliates, such as investment advisory and brokerage companies.

» The board is ultimately responsible for any financial loss or reduction in shareholder value suffered by the bank. Because of the fiduciary nature of many asset management activities and the standards to which fiduciaries are generally held, directors should use prudence in their oversight of these activities to ensure that applicable fiduciary laws and principles are not violated. If, through their failure to exercise prudent oversight, losses accrue to account principals, beneficiaries, or the bank, directors can be held liable for such losses in an action for damages.

» Key responsibilities of the board and senior management relating to asset management activities include the following:

- Establish the strategic direction, risk tolerance standards, and ethical culture for asset management activities.
- Adopt and implement an adequate and effective risk management system.
- Monitor the implementation of asset management risk-taking strategies and the adequacy and effectiveness of the risk management system in achieving the company's strategic goals and financial objectives.

» The board of directors and senior management should establish a supervisory environment that communicates their commitment to risk management and a sound internal control system. They must establish and guide the strategic direction for asset management activities by approving strategic and financial operating plans.

The goal is to create a risk management culture that promotes strong ethics and an environment of responsibility and accountability that is fully accepted within the banking organization.

» It is critical that the board, its designated committees, and senior management provide effective oversight and monitoring of asset management activities. This responsibility may be assisted through the activities of other risk monitoring functions such as risk management, audit, and compliance groups, but the ultimate responsibility and liability rests with the board and senior management.

b. Asset Management Operations and Controls

» The board must establish the bank's strategic direction and risk tolerances. In carrying out these responsibilities, the board should approve policies that set operational standards and risk limits.

- The board should approve well-defined policies commensurate with the nature, size, and complexity of the bank's Asset Management activities. Policies should set standards and may recommend courses of action.
- The board should approve policies, procedures, and monitoring systems designed to ensure that a bank's Asset Management activities comply with applicable laws and regulations.
- In addition, examination procedures include determining whether the board has adopted policies for Asset Management that incorporate internal controls, new product approvals, and audit.

» Examination procedures include determining whether the board or its designated committee has approved and periodically reviewed:

- Strategic plan, strategic direction, and budgeting process for Asset Management operations.
- Organizational structure of the Asset Management business, including delegation of the Asset Management operational activities to designated persons or committees.

» Examination procedures include determining whether the types and frequency of MIS reports (including specific types of reports described in the guidance) provided to the board and management to oversee Asset Management operations are adequate.

» Examination procedures include determining the effectiveness of the board and management's oversight of credit risk associated with Asset Management operations.

» The board should ensure that its internal audit program provides an objective and independent review of Asset Management activities, internal controls, and management information systems.

» Management and the board of directors should ensure that there is a framework of policies, procedures, and workflows that establish effective internal control in all phases of Asset Management operations. 12 C.F.R. 30, Appendix A, "Interagency Guidelines Establishing Standards for Safety and Soundness," sets forth general operational and managerial standards for internal controls and information systems as well as internal audit systems that are applicable to both fiduciary and non-fiduciary accounts.

» 12 U.S.C. 161 requires board attestation of reports of condition, including Consolidated Reports of Condition and Income Schedule RC-T "Fiduciary and Related Services."

» The board is responsible for overseeing business continuity planning for all business lines, including Asset Management. The board should review and approve the bank's contingency plans annually.

» 12 C.F.R. 30, Appendix B, "Interagency Guidelines Establishing Standards for Safeguarding Customer Information," requires that the board of directors, or appropriate committee of the board, approve the bank's information security program and oversee the program's development, implementation, and oversight.

» 12 C.F.R. 9.13 specifically requires that a national bank place assets of *fiduciary* accounts in the joint custody or control of no fewer than two of the fiduciary officers or employees who have been designated for that purpose by the board of directors.

» Vault custodians for fiduciary assets must be specifically designated by either name or title by the board of directors in accordance with 12 C.F.R. 9.13.

» The board is responsible for approving adequate safeguards and controls to maintain fiduciary assets off-premises, in accordance with 12 C.F.R. 9.13.

» BSA/AML compliance programs must be written, approved by the board of directors, and noted in the board minutes.

» Pursuant to 12 C.F.R. Part 225, Subpart B, the acquisition of voting control of bank or bank holding company securities generally requires an application. However, an acquisition of voting securities by a bank or bank holding company in good faith and acting in a fiduciary capacity is generally excluded from this requirement except that:

- in the event that the fiduciary has sole discretionary authority to vote the securities, and it retains the securities and the authority to vote the securities for more than two years, the fiduciary must then obtain board approval to hold the securities; or

- in the event that the fiduciary acquires the securities for the benefit of the acquiring bank or other company, or its shareholders, employees, or subsidiaries, the fiduciary must obtain board approval to hold the securities.

» In overseeing IT systems used by Asset Management, the board and management should ensure that:

- the systems and technology support the bank's strategic goals and objectives for Asset Management and have the capacity to support current and anticipated transaction volumes and product complexity;

- the information and reports provided by these systems are timely, accurate, reliable, consistent, complete, and relevant;

- bank and customer information are adequately protected from unauthorized disclosure or alteration and are available when needed; and

- business resumption and contingency plans are adequate, and data retention requirements are met.

» Examination procedures include determining whether senior management and the board of directors or a committee of the board are involved in the approval process for outsourcing decisions and servicer selection.

» This section of the Comptroller's Handbook notes that the use of the name of a nominee partnership for securities registration facilitates timely trade settlements and streamlines securities servicing. It further states that, in connection with the use of such a nominee partnership, boards of directors typically authorize the execution of a nominee partnership agreement between designated officers or employees of the bank and the bank itself.

c. Agricultural Lending

The board should establish adequate policies appropriate for the complexity and scope of the bank's agricultural lending activities.

The board should annually review and approve the agricultural loan policies. Examination procedures include determining whether the board:

» evaluates existing policies to determine whether they are compatible with market conditions;

» updates stress-testing requirements for borrowers, including the minimum loan size that will require management to perform stress tests on an individual borrower;

» reviews stress-testing policy on the entire agricultural loan portfolio and on individual related segments of the agricultural portfolio; and

» ensures policies are consistent with the bank's strategic direction and risk appetite.

The board is responsible for ensuring control systems are implemented to monitor compliance with established agricultural lending policies.

Bank management should also provide the board an analysis of the risk posed by agricultural lending activities, as well as risks correlated to the agricultural industry and their potential effects on the bank's asset quality, earnings, capital, and liquidity.

» Examination procedures include determining whether management has clearly communicated objectives and risk limits as a percentage of total capital for the agricultural portfolio to the board of directors and whether the board has approved these goals.

» Examiners also should consider whether management and the board receive appropriate reports to analyze and understand the effect of agricultural activities on the bank's credit risk profile, including off-balance-sheet activities.

The board, management, and agricultural lending staff should possess sufficient technical expertise corresponding to the volume and complexity of the bank's agricultural portfolio. Board planning for staff retention and management succession is critical. The board should ensure that the bank's agricultural loan officers are sufficient in number to grant and administer credits in accordance with the bank's policy.

The board should ensure that the internal audit functions are independent of agricultural loan production, approval, and credit administration functions.

d. Allowance for Loan and Lease Losses

» Examination procedures include determining whether the board has established an adequate policy governing the allowance for loan and lease losses, which should provide for the following:

- A comprehensive and well documented process for maintaining an adequate allowance.
  - *Bank management must evaluate the adequacy of the allowance at least quarterly and report its findings to the board of directors before preparing the bank's report of condition and income.*
- An effective loan review system that will identify, monitor, and address asset quality problems in an accurate and timely manner.
- Procedures for the timely charge off of loans that are determined to be uncollectible.
  - *Examination procedures include determining whether all loans charged off are reviewed and approved by the board of directors as evidenced by the minutes of board meetings.*
- Defined collection efforts to be continued after a loan is charged off.

» *See also* Interagency Policy Statement on the Allowance for Loan and Lease Losses described below.

e. Asset-Based Lending

» Asset-based lending policies should be in writing and

initially and periodically reviewed and approved by a bank's board of directors. At a minimum, the policies should address:

- ABL goals, objectives, and risk limits and expectations;
- loan approval requirements that mandate senior-level oversight;
- staff responsibilities for establishing and maintaining sound underwriting standards and prudent credit risk management standards;
- standards for liquidity and collateral monitoring, advance rates, field audits, and loan covenants;
- pricing policies that ensure a prudent trade-off between risk and reward; and
- management's requirement for action plans to use when conversion cycles, collateral values (quality of the borrowing base), or operating cash flow decline significantly from projections. These should include remedial initiatives and triggers for risk-rating changes, changes to accrual status, and loss recognition.

» The OCC expects banks and their boards of directors to properly oversee and manage third-party relationships, in accordance with Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance."

» Examination procedures include determining whether the board of directors has clearly communicated objectives and risk limits for ABL to the bank's management and staff.

» Examination procedures include determining whether management and the board receive appropriate reports to analyze and understand the impact of ABL activities on the bank's credit risk profile, including off-balance-sheet activities.

f. Asset Securitization

» If the bank is the seller/originator in a securitization, the FDIC in its *Statement of Policy regarding Treatment of Security Interests after Appointment of the FDIC as Conservator or Receiver* (58 FR 16833, March 31, 1993) has stated that the FDIC as conservator or receiver would not seek to void an otherwise legally enforceable and perfected security interest, provided that the security agreement evidencing the security interest is in writing, was duly approved by the board of directors of the bank or its loan committee, and remains an official record of the bank.

» Examination procedures include determining whether the board has approved the bank's securitization business plan, which should include, at a minimum, the following:

- The integration of the securitization program into the bank's corporate strategic plan.
- The integration of the securitization program into the bank's asset/liability, contingency funding, and capital plans.
- The integration of the securitization program into the bank's compliance review, loan review, and audit program.
- The specific capacities in which the bank will engage (servicer, trustee, credit enhancer, etc.).
- The establishment of a risk identification process.
- The type(s) and volume of business to be done in total (aggregate of deals in process as well as completed deals that are still outstanding).
- Profitability objectives.

» Examination procedures include determining whether the bank's securitization policies address minimum MIS reports to be presented to senior management and the

board or appropriate committees. (During reviews of applicable meeting minutes, examiners should ascertain which reports are presented and the depth of discussions held.)

» Examination procedures include determining whether the board of directors or appropriate committee and management have a separate securitization steering committee. If so, examiners should review committee minutes for significant information.

» Examination procedures include ensuring that the board or an appropriate committee reviews incentive plans covering personnel involved in the securitization process, and determining whether these plans are oriented toward quality execution and long-run profitability rather than high volume, short-term asset production and sales.

» Examiners also should determine whether senior management and the board of directors are aware of any substantial payments or bonuses made under these plans.

g. Bank Dealer Activities

» Examination procedures include determining the extent and effectiveness of trading policy supervision by, among other things:

- Reviewing the abstracted minutes of the board of directors meetings and/or of any appropriate committee; and
- Evaluating the sufficiency of analytical data used in the most recent board or committee trading department review.

» Examination procedures include determining whether the board of directors, consistent with its duties and responsibilities, has adopted written securities underwriting/trading policies that meet the comprehensive criteria set forth in the guidance.

- Examination procedures also include determining whether the underwriting/trading policies are reviewed at least quarterly by the board to determine their adequacy in light of changing conditions, and whether there is a periodic review by the board to assure that the underwriting/trading department is in compliance with its policies.

» Examination procedures include determining whether the board of directors has adopted written offsetting repurchase transaction policies that meet the comprehensive criteria set forth in this section of the Comptroller's Handbook.

h. Bank Premises and Equipment

» After real estate acquired for future expansion has been held for one year, a board resolution detailing plans for its use must be available for inspection.

» For any bank premises transactions involving insiders or affiliates, examination procedures include determining whether they are at arms-length, reasonable, approved by the board of directors, and in compliance with *12 U.S.C. 371c* for affiliates and *12 U.S.C. 375* for insiders.

» Examination procedures include determining whether the bank's policies regarding bank premises and equipment:

- are approved by the board or a designated committee,
- are reviewed and updated at least annually by the board, and
- include the requirement that the board must give prior approval for all major fixed asset sales and disposals.
    - *Separately, examination procedures include determining whether the approval of the board of directors, or its designated committee, is required for all major additions, sales,*

or disposals of property (if so, determine the amount that constitutes a major addition, sale, or disposal).

i. Trade Finance and Services

» A bank's trade policy should have a board- or board committee-approved risk appetite statement that clearly communicates the amount of risk as a percentage of capital that the bank is willing to take in pursuing its strategic objectives in trade finance and services activities.

- The policy should, for example, identify the products, target markets, prospective customers, and desirable countries. It also should set limits, documentation requirements, and parameters for monitoring and reporting.

- Examination procedures include determining whether the board of directors periodically reviews and approves the bank's trade policies.

» The board of directors and management should receive timely, accurate, and useful information, including exceptions reporting, to evaluate the risk levels and performance of the trade business.

» Consistent with OCC Bulletin 2010-24, "Interagency Guidance on Sound Incentive Compensation Policies," the bank's incentive compensation program should be approved by the board of directors and comply with three key principles: (1) provide employees with incentives that appropriately balance risk and reward; (2) be compatible with effective controls and risk management; and (3) be supported by strong corporate governance, including active and effective oversight by the organization's board of directors. The program should be reviewed regularly to ensure its effectiveness.

» Examination procedures include determining whether, as applicable, the board of directors has adopted policies to control and monitor the foreign-exchange transaction and translation risk arising from discounting foreign-currency denominated drafts and acceptances and foreign operations.

j. Capital Accounts and Dividends

» For a dividend to be declared, the board of directors must take formal action to designate the medium of payment, the dividend rate, the shareholder record date and date of payment.

» The board of directors should ensure that any proposed dividend is consistent with the bank's projections, capital plan and strategic plan, and will not have an adverse impact on the bank's long-term capital adequacy.

» Examination procedures include determining whether the board has adopted formal or informal capital and dividend polices that:

- require a separation of duties between preparation of call reports (Schedule RC-R) and audits of the process;

- address the size of the institution and the nature of its activities to ensure an adequate level of capital is maintained as well as an appropriate level of dividends;

- require management approval regarding the risk weighting of unusual assets; and

- prohibit the signing of blank stock certificates.

» Examination procedures include determining whether clear lines of authority and responsibility for monitoring adherence to policies, procedures, and limits have been established by the board and senior management.

» Examination procedures include determining whether the board has passed a resolution that designates the officers who have the authority to sign stock

certificates, maintain custody of unissued stock certificates, sign dividend checks and maintain stock journals and records.

» Examination procedures include determining whether the board and management possess the knowledge required or engage competent personnel to address capital and dividend issues.

k. Cash Accounts

» Examination procedures include determining whether all cash items are reviewed at least monthly by the board of directors or an appropriate designee, and whether cash items recommended for charge off are reviewed and approved by the board of directors, a designated committee thereof, or an officer with no operational responsibilities.

l. Deposit-Related Credit

» The board and management of any bank considering whether to offer DRC products and services or to maintain or expand the bank's DRC program should be fully aware of the risks involved.

» The board and management should limit the bank's volume of DRC relative to the bank's capital, its risk profile, and management's ability to monitor and control DRC risks.

» A bank's use of a third party, including technology service providers, to provide products and services does not diminish the responsibility of the bank's board of directors and management to ensure that the activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations, just as if the bank were to perform the activities in-house.

» Examination procedures include determining whether:

- DRC policies are approved and annually reviewed by the board of directors or a committee thereof;
- the board, or a committee thereof, evaluates policies for changing market and business conditions at least annually;
- DRC policies require adequate MIS to keep management and the board informed of the DRC program's condition;
- the board has adopted a policy applicable to small businesses for underwriting new DRC accounts, or determining eligibility criteria for overdraft protection. If so, examiners should determine whether the policy meets the criteria specified in the guidance;
- audit findings and the status of responses to audit findings are relayed to the board;
- the information and reporting the directors receive is timely, accurate, and useful. At a minimum, reports should include information for each portfolio product, number of accounts and total balances, delinquency and charge-off information, fraud activity, and risk levels and trends for the DRC area; and
- credit limit approvals are made by an officer or employee granted credit authority by the board of directors.

m. Collective Investment Funds

» A bank's board of directors must manage or direct a collective investment fund's ("CIF") administration. A board may assign fiduciary management authority to any director, officer, employee, or committee of the bank and may use the qualified personnel and facilities of its affiliates to fulfill its fiduciary responsibilities (*see* 12 CFR 9.4 for national banks and 12 CFR 150.150 for FSAs). Management must ensure that all aspects of a bank-administered CIF comply with applicable law. Management

must take special precautions to ensure that procedures are in place to prevent a bank employee, an agent for the bank, or an agent for an EB plan from investing ineligible assets in a CIF. These precautions are particularly important when access to a fund may be available to persons outside of the bank through trading platforms such as the National Securities Clearing Corporation's Fund/SERV.

» The board may purchase administrative services for a CIF from a third-party vendor. A bank that does so must ensure that it complies with the "exclusive management" requirement set forth in 12 CFR 9.18(b)(2), which allows for prudent delegation to others, as well as with applicable interpretations of the '40 Act.

» If the board uses the services of a third-party vendor, such as an RIA, the board must ensure that the vendor conducts its services in a safe and sound manner and in compliance with applicable law. The board and senior management must provide proper oversight of those given the authority to administer the CIF, including a third-party vendor.

» The board and senior management are responsible for ensuring that the CIF risk management system includes sound internal controls and an effective audit program.

» The board must also ensure that each CIF administered by the bank is audited at least once each 12-month period in accordance with 12 CFR 9.18(b)(6).

n. Commercial Loans

» Examination procedures include determining whether:

- the board has adopted commercial lending policies consistent with safe and sound banking practices and apvpropriate to the size, nature, and scope of the bank's operations, including policies that:
  - *establish procedures for reviewing credit applications;*
  - *establish standards for determining credit lines;*
  - *define acceptable collateral;*
  - *establish standards for determining loan-to-value parameters;*
  - *establish minimum requirements for verification of borrower's assets;*
  - *establish minimum standards for documentation; and*
  - *establish minimum standards for monitoring, measuring, and reporting identified risks and associated controls.*
- management and the board monitor changing market conditions in the bank's lending area to ensure that lending policies continue to be appropriate; and
- the bank's commercial lending policies are reviewed and approved by the board of directors at least annually.

o. Commercial Real Estate Lending

» Pursuant to Subpart D of 12 C.F.R. Part 34, the board must review and approve the bank's real estate lending policies at least annually.

- An appropriate environmental risk management program should reflect the level and nature of the bank's real estate lending activities, its risk profile, and consideration of applicable environmental laws.
- The program, as well as the bank's lending policies, should be reviewed and approved annually by the bank's board of directors or a designated committee of the board.

» *See also* Concentrations in Commercial Real Estate Lend-

ing, Sound Risk Management Practices described below.

p. Community Bank Supervision

» In all banks, the board of directors and management are required to monitor compliance with BSA/AML and Office of Foreign Assets Control ("OFAC") laws and regulations, as well as all applicable consumer protection laws and regulations. The board is responsible for creating a strong compliance culture within the bank that includes management accountability.

» Examination procedures include determining the quality of board or audit committee oversight of the bank's audit programs, including with respect to a number of criteria specified in the guidance.

» Examination procedures include determining the adequacy of management and board oversight in a number of areas, including with respect to risk management, staff selection, insurance policies, capital, liquidity, investment portfolio activities, market risk, IT, asset management, and consumer compliance.

q. Compliance Management System

» Compliance with law and regulation must be managed as an integral part of any bank's business strategy. The board of directors and management must recognize the scope and implications of laws and regulations that apply to their bank. They must establish a compliance management system that not only protects the bank, but also uses resources effectively and minimizes disruptions in daily activities.

» To ensure an effective approach to compliance, the board and management should make compliance a high priority. The participation of senior management in the development and maintenance of a compliance program is essential.

» The board and senior management periodically should review the effectiveness of its compliance management system. This review should include reports which identify any weaknesses or required modifications due to changes in laws, regulations, or policy statements.

» Examination procedures to evaluate the quality of the bank's compliance management system include determining the quality and effectiveness of board and senior management supervision and administration of the bank's compliance management system.

» Examination procedures include evaluating the level of supervision of consumer compliance (except Community Reinvestment Act) provided by the board of directors by reviewing board minutes and board reports, and through discussions with management. Consider the extent and frequency to which the board:

- Approves the compliance management system.
- Approves bank-wide policies and procedures that address consumer protection laws.
- Considers the staffing, compensation, and budgetary needs of the compliance program.
- Reviews the effectiveness of the compliance management system.
- Assesses and monitors the risks associated with the bank's consumer compliance activities.

» Examination procedures include reviewing reports provided to the board concerning compliance issues to identify significant or unresolved deficiencies and determine whether the reports allow the board to determine if policies are followed and corrective action is taken when complaints, compliance reports, internal/external audit reports, or the compliance officer indicates that action is necessary.

r. Concentrations of Credit

» This section of the Comptroller's Handbook emphasizes the need for boards of directors to ensure that management effectively implements internal processes designed to identify, measure, monitor, and control concentrations of credit.

» This section further states that the OCC expects banks to implement board-approved policies and procedures appropriate to the size and complexity of their portfolios.

» Bank management should provide the institution's board of directors with an analysis of the risk posed by credit concentrations as well as their potential effect on the bank's asset quality, earnings, capital and liquidity.

- Examination procedures include determining whether the bank has established a process for using stress testing results to identify potential credit concentrations and to evaluate the potential impact of adverse scenarios on credit concentrations on the bank's capital and liquidity, and for reporting those results to senior management and the board of directors.

s. Conflict of Interest

» An effective risk management system is characterized by an active board of directors and senior management supervision and sound processes for risk assessment, control, and monitoring. A bank's board of directors and senior management should establish and promote an appropriate corporate culture that includes the adoption of a code of ethics that, among other things, sets forth general expectations for ethical behavior and compliance with banking and applicable securities laws.

» A bank's board of directors is ultimately responsible for the administration of its fiduciary activities. A bank's risk management system should comprehensively address conflicts of interest in the administration of fiduciary and other asset management accounts.

- National banks are required under 12 CFR 9.5 to adopt and follow written policies and procedures adequate to maintain the bank's fiduciary activities in compliance with applicable law. These should include policies and procedures related to conflicts of interest and self-dealing, the use of material inside information, and brokerage placement practices.

- The board of directors should adopt strong written policies that closely govern the relationship between related parties and interests and fiduciary accounts, and should ensure that management implements a process to monitor and validate compliance with these policies.

» A bank's risk management processes should require that exceptions to bank policy or exceptions that are in excess of the bank's risk appetite are identified and escalated to a designated committee of the board of directors responsible for fiduciary oversight or a designated senior manager for resolution or approval.

» A bank's MIS should effectively provide management and the board of directors with timely, accurate, and pertinent information about the nature and scope of actual and potential conflicts of interest arising from the bank's asset management activities. A bank's MIS and related processes should enable management and the board to effectively:

- determine whether specific conflicts or potential conflicts are permissible under applicable law and consistent with the bank's policies and risk appetite.

- monitor and ensure appropriate resolution of conflicts of interest that are either impermissible or inconsistent with the bank's policies or risk appetite.

- monitor potential conflicts of interest and self-dealing.

- evaluate the level of risk to the bank from conflicts of interest.

- determine the bank's aggregate risk from conflicts of interest in asset management products and services.

» In ensuring that a suitable fiduciary audit is performed in accordance with 12 CFR 9.9, the board of directors must assess whether the audit programs in place are adequate to determine whether conflicts of interest are managed in accordance with applicable law and with bank policies and procedures.

t. Consigned Items and Other Customer Services

» Examination procedures include determining whether the bank has formal/informal policies adequate to control the risks from consigned items and other customer services, and whether the policies have been adopted by the board of directors.

u. Country Risk Management

» The board of directors must ensure that country risk is managed effectively.

- This section specifically notes here that, depending on bank size and complexity, the board of directors may delegate board functions to board committees. *See* Chapter II of the OCC's *Directors' Book* in the National Bank Directors' Toolkit.

» The board is responsible for periodically reviewing and approving policies governing the bank's international activities to ensure that they are appropriate and consistent with the bank's strategic plans, goals, risk tolerance, and strength of capital and management.

- Country risk limits should be approved by the board of directors and communicated to all affected departments and staff. They should be reviewed and approved at least annually and more frequently when concerns about a particular country arise.

  - *Exceptions to country exposure limits should be reported to an appropriate level of management or to the board so they can be approved or corrective measures considered.*

- Where the bank uses economic or regulatory capital to control and manage country exposure, the board should evaluate and approve the allocations.

- Also, through appropriate reporting processes, the board should evaluate how effectively bank management controls country risk.

  - *Bank policies and procedures should require periodic reporting of country risk exposures and limit exceptions to senior management and the board of directors.*

  - *If the level of foreign exposures in the bank is significant, or if a country to which the bank is exposed is considered to be high risk, exposures should be reported to the board at least quarterly. More frequent reporting is appropriate when there are concentrations or deterioration in foreign exposures would threaten the earnings, capital, and/or reputation of the bank.*

  - *Banks should periodically stress-test their foreign exposures and report the results to their boards of directors and senior management*

» The bank's board of directors and senior management should ensure that the country risk management process includes effective internal control processes.

v. Credit Card Lending

» If accounts routinely exceed credit limits, then the bank's board or management should be concerned

either with the initial line assignment or with the risk management process.

» Examination procedures include:

- determining whether credit card lending policies were approved by the board of directors at inception and included in annual policy reviews thereafter.
- Reviewing meeting minutes from the board of directors or designated committee overseeing credit card activities (the IT examiner should coordinate this review with the credit card lending EIC).
- Evaluating the adequacy of the bank's test process for new credit card products, associated marketing campaigns, and other significant initiatives. Review the process to determine whether testing includes a thorough and well-supported postmortem analysis in which results are presented to and approved by senior management and the board before full rollout.
- determining whether the board or senior management reviewed and approved the incentive pay program before implementation.

» The Internal Control Questionnaire includes determining whether the board or a board committee (depending on the risk profile of the bank), consistent with its duties and responsibilities, adopted (and reviewed at least annually to determine whether they are compatible with changing market conditions and the bank's strategic plan) written policies that establish: procedures for reviewing credit card applications; standards for determining credit lines; minimum standards for documentation; standards for collection procedures; and third-party relationship management.

w. Due from Banks

» Examination procedures include determining whether the board of directors, consistent with its duties and responsibilities, has adopted written policies for due from bank accounts that:

- Provide for the periodic review and approval of balances maintained in each such account.
- Indicate person(s) responsible for monitoring balances and the application of approved procedures.
- Establish levels of check-signing authority.
- Indicate officers responsible for approval of transfers between correspondent banks and include procedures for documenting such approval.
- Indicate the supervisor responsible for regulatory review of reconciliations and reconciling items.
- Indicate that all entries to the accounts are to be approved by an officer or appropriate supervisor and that such approval will be documented.
- Establish time guidelines for the charge-off of old open items.
- Establish procedures for entering into revocable reserve account charge agreements.

» Examination procedures include determining whether the board reviews these policies at least annually to determine their adequacy in light of changing conditions. The board, and management, should establish effective processes for managing the risks associated with due from bank accounts

x. Emerging Market Country Products and Trading Activities

» The board, a committee thereof, or appropriate management as designated by the board, should ensure

that EM activities are consistent with the overall business strategy of the bank, which entails the development and implementation of a sound risk management framework composed of appropriate written policies and procedures, effective risk measurement and reporting systems, and independent oversight and control processes.

» The board or a committee thereof should review EM policies at least annually.

» The board or a committee thereof should track management's responses to audit and risk control findings regarding EM to correct any deficiencies.

» The board and management should use limits and exposure measurement systems to provide a means of control over aggregate EM exposure and to foster communication of changes in trader activities, market values, and the bank's overall risk profile.

» The board or a committee thereof should approve at least annually, or as market conditions warrant, aggregate risk-taking limits with respect to EM exposure.

y. Floor Plan Lending

» A bank's board of directors should periodically review and approve floor plan lending policies and procedures as appropriate for the bank's floor plan lending activities. The board should assess whether the internal audit and loan review functions perform timely reviews of this area and are independent of floor plan lending approval and credit administration functions. The board should also periodically review appropriate management information system (MIS) reports regarding the institution's floor plan lending activities to better fulfill its oversight role.

» Internal loan review personnel should discuss any deficiencies within the floor plan lending department with management and the board of directors.

» Examination procedures include determining whether:

- the board has adopted adequate and effective policies that are consistent with safe and sound banking practices and appropriate to the size, nature, and scope of the bank's floor plan lending activities;
- the board, consistent with its duties and responsibilities, periodically reviews and approves the bank's floor plan lending policies as appropriate and whether the review and approval process adequately considered changing market conditions, regulatory changes, and the bank's risk appetite and loan strategies; and
- the board or senior management has established adequate procedures for ensuring compliance with applicable laws and regulations related to floor plan lending.

z. Foreign Exchange

» Examination procedures include determining whether the board has adopted written policies governing trading limits; segregation of duties among traders, bookkeepers, and confirmation personnel; accounting and revaluation procedures; and management accounting procedures.

aa. Futures Commission Merchant Activities

» It is incumbent upon the bank's board and senior management to understand the role the futures commission merchant operating subsidiary plays within the overall business strategies of the bank and the mechanisms used to manage risks.

» To fulfill its responsibilities, the bank's board must ensure that appropriate written policies and strong control processes are guiding the actions of the FCM's management.

- The bank's board must endorse written corporate policies that provide a framework for the management of risk.

- The board should ensure that the policy framework identifies managerial oversight, assigns clear responsibility, and requires the development and implementation of sufficiently detailed procedures to guide the FCM's daily activities.

- Policies should detail the type and nature of the activity authorized, articulate the risk tolerance to the bank through comprehensive risk limits and require regular, independent risk position and performance reporting.

- The board should review and endorse significant changes to policies. At least annually, the board, or a committee thereof, also should approve key policy statements, particularly those related to risk tolerance limits. Meeting minutes should document these actions.

- The board should approve aggregate risk-taking limits at least once a year, which should be directly related to the nature of the bank's strategies, historical performance, and the overall level of earnings or capital that the board is willing to place at risk.

» The board and senior management must provide adequate resources (financial, technical expertise, and systems technology) to implement effectively the fundamental elements comprising risk management, which are: exposure limit systems, risk measurement capabilities, risk monitoring and reporting mechanisms, and segregation of critical operational and control processes.

» The board and management should assess the FCM's vulnerability to each risk associated with futures and options activities, on an ongoing basis, in response to changing circumstances.

» The board and senior management should use limits and exposure measurement systems to foster communication of changes in the FCM's overall risk profile.

» If a bank establishes a FCM operating subsidiary to broker trades for the bank and other related entities, it is incumbent upon bank senior management and the board to establish a control framework to ensure accurate monitoring of transactions between affiliates and the FCM.

- The board and senior management should establish policies and procedures that address FCM transactions for affiliates.

  - *At a minimum, the policy should describe the nature of acceptable affiliate transactions and require that transactions for customers take priority over the interests of the FCM and its affiliates.*

  - *Senior management should ensure that affiliate transactions comply with such policy.*

» The bank's board should ensure that the management of the FCM possesses the necessary experience in futures trading, brokerage, and operations activities. The board and senior management should ensure that adequate resources are dedicated to the FCM for staffing, technical, and operational needs.

bb. Insider Activities

» The board of directors must demonstrate leadership by ensuring a culture that does not tolerate unethical behavior or circumvention of regulations, and by adopting and administering strong written policies that closely govern the relationship between a bank and all insiders.

- The board must adopt and enforce strong written insider policies governing the bank's relationship to insiders and their related interests.

- The board must also ensure that bank management implements a process to monitor and validate compliance with these policies. The bank's board and management are responsible for ensuring that the bank complies with laws, regulations, prescribed practices, and ethical standards.

- *The board, through its oversight role, should ensure that the bank's system of internal controls and audit alerts the bank to the following practices or conditions: transactions resulting in a conflict of interest or the appearance of such a conflict; the payment of excessive compensation, unjustified fees, or compensation that encourages inappropriate risk-taking that could lead to material financial loss; failure to comply with applicable insider laws, regulations, or bank-imposed restrictions; and other red flags for possible insider fraud.*

- *If any of these practices is discovered, the board should determine the cause, instruct management to take appropriate corrective action, and oversee necessary revisions to policies or internal controls.*

» The board and management must ensure that their business and personal relationships with the bank are always at arm's length, do not bias decisions or otherwise harm the bank, and do not improperly take business opportunities away from the bank. In addition, the board and management must take reasonable action to prevent other employees from abusing their positions within the bank. In this regard, the board and management have a number of duties relating to insider activities:

- Establishing appropriate insider policies, including a code of ethics and required disclosures of actual and potential conflicts of interest.

- Establishing and applying sound, independent processes to monitor and ensure compliance with insider policies, laws, and regulations, e.g., providing for effective internal controls and adequate audit and compliance coverage.

- Fulfilling fiduciary obligations, including the duty of care and the duty of loyalty.

- Complying with insider-related laws and regulations.

- Ensuring that hiring practices require disclosure of and address potential conflicts of interest and insider transactions.

- Ensure adequate training of board, management, and staff regarding insider policies and laws.

- Setting appropriate compensation and fees paid to insiders.

- Following prudent dividend policies.

- Implementing sound management information systems that transparently and comprehensively report on insider risk activities and exposures.

- Submitting accurate financial reports and other disclosures.

» The board is responsible for reviewing and closely monitoring all insider incentive compensation arrangements to ensure that they do not result in any unreasonable risk-taking to the bank and to ensure compliance with regulations and guidance.

- If excessive management or other fees are paid to insiders, the board is responsible for taking corrective action, possibly to include seeking restitution from the insider.

cc. Installment Loans

» Examination procedures include:

- determining whether the board of directors, consistent with its duties and responsibilities, has adopted informal (unwritten) or formal (written) installment loan policies that establish: procedures for reviewing and approving installment loan applications; underwriting standards for each type of installment product offered; and minimum documentation standards; and

- determining whether the board approves installment

lending policies annually and whether they evaluate existing installment loan policies to determine if they are compatible with changing market conditions and laws and regulations.

dd. Insurance Activities

» The board and senior bank management should develop and implement effective risk management processes that effectively assess, control, and monitor the risks emanating from a bank's insurance activities.

» A bank's board of directors is responsible for overseeing insurance activities conducted directly by the bank or through contractual arrangements with third parties, including bank subsidiaries, affiliates, or unaffiliated providers.

» In carrying out this responsibility, the board should adopt an appropriate program management plan to guide the bank's insurance activities.

» This plan should articulate the board's risk tolerance and establish the necessary systems for controlling the program's risks.

» Annually, the board should reevaluate the plan for appropriateness and effect any necessary changes.

ee. Interest Rate Risk

» It is the responsibility of the board and senior management to understand the nature and level of interest rate risk being taken by the bank and how that risk fits within the overall business strategies of the bank and the mechanisms used to manage that risk. The board has four broad responsibilities; it must:

- Establish and guide the bank's strategic direction and tolerance for interest rate risk and identify the senior managers who have the authority and responsibility for managing this risk.
    - *The bank's board of directors should set the bank's tolerance for interest rate risk and communicate that Based on these tolerances, senior management should establish appropriate risk limits that maintain a bank's exposure within the board's risk tolerances over a range of possible changes in interest rates.*
- Monitor the bank's performance and overall interest rate risk profile, ensuring that the level of interest rate risk is maintained at prudent levels and is supported by adequate capital.
    - *In assessing the bank's capital adequacy for interest rate risk, the board should consider the bank's current and potential interest rate risk exposure as well as other risks that may impair the bank's capital, such as credit, liquidity, and transaction risks.*
- Ensure that the bank implements sound fundamental principles that facilitate the identification, measurement, monitoring, and control of interest rate risk.
- Ensure that adequate technical and human resources are devoted to interest rate risk management.

» Senior management and the board, or a committee thereof, should receive reports on the bank's interest rate risk profile at least quarterly, but more frequently if the character and level of the bank's risk requires it.

- The bank's key behavioral and pricing assumptions (*e.g.*, with respect to estimated prepayments) and their impact should be reviewed by the board, or a committee thereof, at least annually.

» In addition to establishing clear lines of authority, responsibilities, and risk limits, management and board should ensure that adequate resources are provided to support risk monitoring, audit, and control functions.

» A bank's board usually will delegate responsibility for establishing specific interest rate risk policies and practices to a committee of senior managers. This senior management committee is often referred to as the Finance Committee or Asset/Liability Management Committee (ALCO).

ff. Internal and External Audits

[*The following are selected excerpts from this 188-page guidance, which includes references to the "board" over 200 times*]

» The board of directors is responsible and accountable for establishing, overseeing, and maintaining audit functions that: effectively test and monitor internal controls; ensure the reliability of the bank's financial statements and reporting; and satisfy statutory, regulatory, and supervisory requirements.

» Directors must ensure that the audit programs test internal controls to identify inaccurate, incomplete, or unauthorized transactions; deficiencies in the safeguarding of assets; unreliable financial and regulatory reporting; violations of laws or regulations; and deviations from the institution's policies and procedures**.**

» Directors cannot delegate these responsibilities (however, they may delegate the design, implementation, and monitoring of specific internal controls to management and the testing and assessment of internal controls to internal auditors, other bank personnel, or external third parties).

» Board or audit committee minutes should reflect decisions regarding audits, such as external audit engagement terms (including any decision to forgo an external audit), the type of audits to be performed, or why an audit of a particular area is not necessary.

» Directors should be aware of significant risk and control issues for the bank's operations, especially for new products, emerging technologies, information systems, electronic banking, and new or revised laws and regulations.

» The audit committee's responsibilities should encompass:

- Reviewing and approving audit strategies, policies, programs, and organizational structure, including selection/termination of external auditors or outsourced internal audit vendors.
    - *Among other things, the audit committee should formally approve the overall audit plan at least annually. The internal auditor should present any updated audit plan to the audit committee regularly in accordance with established policy (although quarterly is typical).*
- Establishing schedules and agendas for regular meetings with internal and external auditors. The committee should meet at least four times a year.
- Supervising the audit function directly to ensure that internal and external auditors are independent and objective in their findings.
- Working with internal and external auditors to ensure that the bank has comprehensive audit coverage to meet the risks and demands posed by its current and planned activities.
- Significant input into hiring senior internal audit personnel, setting compensation, reviewing annual audit plans/schedules, and evaluating the internal audit manager's performance.
- Retaining auditors who are fully qualified to audit the kinds of activities in which the bank is engaged.
- Meeting with bank examiners, at least once each supervisory cycle, to discuss findings of OCC reviews, including conclusions regarding audit.
- Monitoring, tracking, and where necessary, providing

discipline to ensure effective and timely response by management to correct internal control weaknesses and violations of law or regulation noted in internal or external audit reports or in examination reports.

» Audit findings are to be properly reported to the board of directors or its audit committee and appropriate bank management; significant matters should be reported directly to the board or its audit committee and senior management.

- To maintain independence, the person responsible for accomplishing the internal audit function should be independent of whatever area is being audited and should report findings directly to the board or its audit committee.
- The auditors should perform follow-up activities promptly and report the results to the board of directors or its audit committee.
- If a third party vendor conducts the audit, the vendor shall jointly, with the internal auditor, report significant findings to the board of directors or its audit committee.

» An independent accountant should send a letter to the board of directors or audit committee that addresses the purpose and scope of the external auditing work to be performed, the period of time to be covered by the audit and other information.

» Results of outsourced work must be well documented and reported promptly to the board of directors or its audit committee by the internal auditor, vendor or both jointly.

» Pursuant to 12 C.F.R. 9.9, if a national bank adopts a system of continuous fiduciary audits, at least once during each calendar year the board of directors' minutes must note the results of all discrete audits performed since the last audit report including significant actions taken as a result of the audits.

» For national banks with securities registered under the Securities Exchange Act of 1934, OCC examiners will determine if, as required by SEC regulations (*see* 17 C.F.R. 229.407(d)), an audit committee report is made which states whether the audit committee reviewed and discussed audited financial statements with management.

» The audit committee of the board is responsible for identifying at least annually the risk areas of the institution's activities and assessing the extent of external auditing involvement needed over each area; the audit committee should report its findings periodically to the full board of directors.

» Examination procedures include considering whether (among other things):

- The board of directors or its audit committee reviews and approves audit programs and policies at least annually.
- The board of directors or its audit committee monitors the implementation of the audit program and associated audit schedules.
- Audit findings are promptly communicated to the board of directors or its audit committee and appropriate bank management.
- The board and management properly follow up on the results of audits and appropriately monitor any significant issues.

» The board of directors or audit committee performed sufficient due diligence to satisfy themselves of any applicable vendor's competence and objectivity prior to entering an outsourcing arrangement.

gg. Internal Control

» A bank's board of directors and management are responsible for establishing and maintaining effective

internal control that meets statutory and regulatory requirements and responds to changes in the bank's environment and conditions.

- The board and management must ensure that the system operates as intended and is modified appropriately when circumstances dictate.

- They also must make sure that the bank's information systems produce pertinent and timely information in a form that enables employees, auditors, and examiners to carry out their respective responsibilities.

- The board must ensure that senior management regularly verifies the integrity of the bank's internal control.

» The board of directors, which oversees the control system in general, approves and reviews the business strategies and policies that govern the system.

- The board also is responsible for understanding risk limits and setting acceptable ones for the bank's major business activities, establishing organizational control structure, and making sure senior management identifies, measures, monitors, and controls risks and monitors internal control effectiveness.

- The board should:

  - *discuss periodically the internal control system's effectiveness with management;*

  - *review internal control evaluations conducted by management, auditors, and examiners in a timely manner;*

  - *monitor management's actions on auditor and examiner internal control recommendations and concerns; and*

  - *periodically review the bank's strategy and risk limits. In some banks, the board of directors delegates these duties and responsibilities to an audit committee, risk committee, or both.*

» Board and management must consider whether a control system's methods, records, and procedures are proper in relation to the bank's: asset size, organization and ownership characteristics, business activities, operational complexity, risk profile, methods of processing data, and legal and regulatory requirements.

» The board of directors must ensure that management properly considers the risks and control issues of emerging technologies, enhanced information systems, and electronic banking.

hh. Large Bank Supervision

The Introduction to this Section of the Handbook states that "This booket is prepared for use by OCC examiners in connection with their examination and supervision activities. Each bank is different and may present specific issues. Accordingly, examiners should apply the guidance in this booklet consistent with each bank's individual circumstances."

» The board must establish the company's strategic direction, risk appetite, and core values. Setting an appropriate tone at the top is critical to establishing an ethical culture. In carrying out these responsibilities, the board should approve policies that set operational standards and risk limits. Well-designed monitoring systems allow the board to hold management accountable for operating within established standards and limits.

» Policies with respect to risk management should be reviewed periodically for effectiveness and approved by the board of directors or a designated board committee.

- Policies are statements of actions adopted by a bank to pursue certain objectives. Policies guide decisions and often set standards (on risk limits, for example) and should be consistent with the bank's underlying mission, risk appetite, and core values. Processes, on the other hand, are the procedures, programs, and practices that impose order on a bank's pursuit of its objectives. Processes define how activities are carried

out and help manage risk. Effective processes are consistent with the underlying policies and are governed by appropriate checks and balances (such as internal controls).

» Examiners must clearly and concisely communicate supervisory concerns to a bank's board and management, allowing management an opportunity to resolve differences, commit to corrective action, and address the concerns. Examiners shall describe the practices that resulted in the concerns, as well as the board's or management's commitment to corrective action, in Matters Requiring Attention ("MRA") in the ROE or in other periodic formal written communications.

» Examiners consider the following assessment factors when making judgments about the quantity of strategic risk. These factors are the minimum standards that all examiners consider during every supervisory cycle to ensure quality supervision. Examiners are required to judge, based on the review of the core assessment factors, whether the risk is low, moderate, or high.

- Board oversight of and engagement on strategic initiatives.
- Board and management's ability to respond to changes in the banking industry and operating environment.
- The quality, integrity, timeliness, and relevance of reports to the board of directors necessary to oversee strategic decisions.

» Examiners consider the following assessment factors when making judgments about the quality of reputation risk management. These factors are the minimum standards that all examiners consider during every supervisory cycle to ensure quality supervision. Examiners are required to judge, based on the review of the core assessment factors, whether risk management is strong, satisfactory, insufficient, or weak.

- The expertise of senior management and the effectiveness of the board of directors in maintaining an ethical, self-policing culture.

ii. Investment Securities

» The responsibility for supervising the bank's investment account rests solely with the board of directors and cannot be delegated to a correspondent bank, an advisory service, a brokerage house, or a rating service.

» The investment portfolio should be reviewed at least annually by the board of directors and quarterly by senior officers of the bank. Sufficient analytical data must be provided to allow the board and senior management to make an informed judgment of the investment policy's effectiveness.

» If a national bank chooses to invest in the shares of an investment company, the bank's investment policy as formally approved by its board of directors should: (1) provide specifically for such investments; (2) require that for initial investments in specific investment companies prior approval of the board of directors be obtained and recorded in the official board minutes; and (3) ensure that procedures, standards, and controls for managing such investments are implemented prior to making the investment.

» The board of directors and/or an appropriate board committee should review and approve a list of securities firms with whom the bank is authorized to do business.

- Purchased securities and repurchase agreement collateral should be kept in safekeeping with selling dealers only when (1) the board is completely satisfied as to the creditworthiness of the securities dealer; and (2) the aggregate value securities held in safekeeping in this manner is within credit limitations that have been approved by the board of directors, or a committee of the board, for unsecured transactions.

- As a part of the process of managing a bank's relationships with securities dealers, the board of directors may also want to consider prohibiting those employees, who are directly involved in purchasing and selling securities for the bank, from engaging in personal securities transactions with the same securities firm the bank uses for its transactions without specific board approval and periodic review. Such prohibition could be included in the bank's code of ethics or code of conduct.

- The board also may want to adopt a policy applicable to directors, officers, or employees concerning receipt of gifts, gratuities, or travel expenses from approved dealer firms and their personnel (*see also* the Bank Bribery Law, 18 U.S.C. 215 and interpretive releases).

» The board of directors should consider any plan to engage in futures, forward, and standby contract activities and should endorse specific written policies in authorizing them.

- Examination procedures include determining whether the board, consistent with its duties and responsibilities, has adopted written investment securities policies, including with respect to when-issued securities, futures, and forward placement contracts, that outline: objectives; permissible types of investments; diversification guidelines, to prevent undue concentration; maturity schedules; limitation on quality ratings; policies regarding exceptions to standard policy; and valuation procedures and frequency.

- Examination procedures also include determining whether investment policies are reviewed at least annually by the board to determine if they are compatible with changing market conditions.

- The board of directors should establish trading limits applicable to futures, forward, and standby contract positions.

  ◦ *Examination procedures include determining whether exceptions from individual limits and gross trading limits are subsequently submitted to the board or an appropriate board committee for ratification.*

- The board, a duly authorized board committee, or the bank's internal auditors should review periodically (at least monthly) contract positions to ascertain conformance with such limits.

- Examination procedures include determining whether weekly reports are prepared for an appropriate board committee which reflect:

  ◦ *all trading activity for the week;*

  ◦ *open positions at the end of the week;*

  ◦ *market value of open positions;*

  ◦ *unrealized gains and losses;*

  ◦ *total trading limits outstanding for the bank; and*

  ◦ *total trading limits for each authorized trader.*

- If the bank is engaged in financial futures contract trading activity, examination procedures include determining whether the board has specifically approved written policies about nonhedging futures contract strategies.

» The acquisition of stripped mortgage-backed securities should be undertaken only in conformance with carefully developed and documented plans prescribing specific positioning and loss limits and control arrangements for enforcing such limits. These plans should be approved by the bank's board of directors and vigorously enforced.

» The international investment portfolio should be reviewed at least annually by the board of directors, and quarterly by senior management, to assure adherence to written policies and procedures.

- Sufficient analytical data must be provided to allow the bank's board of directors and senior management to make informed judgments regarding the effectiveness of the international division's investment policy and procedures.

- Examination procedures include determining whether the board of directors receives regular reports on domestic and international division investment securities, which include valuations, maturity distributions, average yield, and reasons for holding and benefits received (international division and overseas holdings only).

» If the bank is engaged in dollar repos or rolls, examination procedures include determining whether the board has approved the use of dollar repos, and ensuring that the board has authorized particular individuals to conduct dollar repos and that they have sufficient knowledge to do so properly.

» If the bank has due from commercial banks or other depository institutions — time, federal funds sold, commercial paper, securities purchased under agreements to resell or any other money market type of investment, examination procedures include determining whether purchases or sales are reported to the board of directors or its investment committee.

» If the bank holds shares of mutual funds or unit investment trusts, examination procedures include determining whether the board has adopted policies and procedures that include: specific provisions for purchases of mutual fund and unit investment trusts shares; requirements for prior approval of initial investment in investment companies; and procedures standards and controls for managing such investments.

» Examination procedures include determining whether purchases, exchanges, and sales of securities and open contractual commitments are ratified by action of the board of directors or its investment committee and thereby made a matter of record in the minutes.

jj. Lease Financing

» Examination procedures to determine whether the board has adopted effective lease financing policies and practices include:

- Evaluating relevant policies to determine whether they provide appropriate guidance for managing the bank's lease financing and are consistent with the bank's mission, values, and principles. Consider the impact of significant policy changes on the quantity of credit risk, if any. Policies and underwriting guidance should do the following

  - *Establish procedures for reviewing lease financing applications.*

  - *Define types of leasing activities that the bank will consider, including any limits.*

  - *Define qualified property.*

  - *Establish minimum standards for documentation.*

- Determining whether policies establish hard and risk-based limits or positions and delineate prudent actions to be taken if the limits are exceeded.

- Verifying that the board of directors periodically reviews and approves the bank's lease financing policies. Determine whether the board of directors considers the compatibility of the policies with the changing market conditions.

- Testing for compliance with established policies or practices. Identify any area with inadequate supervision or undue risk and discuss with the EIC the need to perform additional procedures

kk. Leveraged Lending

» The board should adopt formal policies that address:

- The definition of leveraged lending and risk objectives.
- Loan approval requirements that require sufficient senior level oversight.
- Responsibilities regarding the establishment of underwriting standards, distribution practices, and credit risk management controls.
- Pricing policies that ensure a prudent tradeoff between risk and return.
- The requirement for action plans whenever cash flow, asset sale proceeds, or collateral values decline significantly from projections. Action plans should include remedial initiatives and triggers for risk rating changes, changes to accrual status, and loss recognition.

» Examination procedures include determining whether:

- the board of directors, consistent with its duties and responsibilities, has established leveraged lending policies appropriate for the complexity and scope of the bank's operations and whether written underwriting guidance addresses important issues not included in board policies;
- annual reviews of leveraged lending policies and underwriting guidance are conducted by the board or an appropriate credit committee; and
- management's response to any material findings by any control group (including audit and loan review) has been verified and reviewed for objectivity and adequacy by senior management and the board (or a committee thereof).

II. Liquidity

» The board should establish sound liquidity risk management policies that include the following critical elements:

- appropriate corporate governance and active involvement by management.
- appropriate strategies, policies, procedures, and limits used to manage and control liquidity risk, even in stressed conditions.
- appropriate liquidity risk measurement and monitoring systems.
- active management of intraday liquidity and collateral.
- maintaining an appropriately diverse mix of existing and potential future funding sources.
- adequate levels of highly liquid marketable securities, with no legal, regulatory, or operational impediments, that can be used to meet liquidity needs in stressful situations.
- comprehensive contingency funding plans (CFP) sufficient to address potential adverse liquidity events and emergency cash flow needs.
- adequate internal controls surrounding all aspects of liquidity risk management.

» The board and senior management should develop and oversee a comprehensive risk management process that identifies, measures, monitors and controls a bank's liquidity risk exposure.

» The board implements policies that govern liquidity risk management under both business-as-usual and stressed conditions. These policies should clearly define the roles and responsibilities of board committees, senior management, and senior management committees with appropriate segregation of duties between execution and oversight of liquidity risk. In multibank holding companies, the board should also understand the liquidity profile of important affiliates and their impact on a bank.

» Examination procedures to assess the adequacy of internal controls surrounding the liquidity risk management process include determining whether the board and senior management have established clear lines of authority and responsibility for monitoring adherence to policies, procedures, and limits.

» Examination procedures include determining whether:

- actions taken by management to deal with material weaknesses have been verified and reviewed for objectivity and adequacy by senior management or the board;
- the board and senior management have established adequate procedures for ensuring compliance with applicable laws and regulations;
- if the bank relies on another party (such as its holding company, a bank rating agency, or another correspondent) to provide financial analysis of a correspondent, the bank's board of directors has reviewed and approved the assessment criteria used by that party;
- if the bank relies on another party to select or monitor its correspondents, the bank's board of directors reviewed and approved the selection criteria used; and
- if the bank relies on a correspondent to choose other correspondents to whom the bank lends federal funds, the bank's board of directors reviewed and approved the selection criteria used.

mm.Litigation and Other Legal Matters

» Examination procedures to determine whether the board and management have established appropriate guidelines for managing the risks of litigation and other legal matters include determining whether the bank's relevant policies are reviewed and approved by the board or a board designated committee.

nn. Loan Portfolio Management

» Senior management and the board should periodically evaluate the bank's credit culture and risk profile.

» With respect to loan portfolio objectives, the board of directors must ensure that loans are made with the following three basic objectives in mind: (i) to grant loans on a sound and collectible basis; (ii) to invest the bank's funds profitably for the benefit of shareholders and the protection of depositors; and (iii) to serve the legitimate credit needs of their communities.

- For most banks, meeting these three objectives will require that senior management and the board of directors develop medium- and long-term strategic plans and objectives for the loan portfolio.

» Senior management and the board are responsible for setting risk limits on the bank's lending activities.

- The bank should have a system in place to ensure that exposures approaching risk limits are brought to the attention of senior management and the board.
- Aggregate exceptions levels should be analyzed regularly and reported to the bank's board of directors.
    - *In addition, "more substantive" exceptions to lending standards should have heightened reporting requirements to senior management and the board.*
- Both senior management and the board of directors should receive clear, concise, timely information about the loan portfolio and its attendant risks.
    - *Reports to the board generally should not contain the same level of detail as those provided to senior management, although in the smallest banks management reports may be sufficient for board use.*
- To ensure the independence of loan review, the loan

review unit should report administratively and functionally to the board of directors or a standing committee with audit responsibilities.

oo. Merchant Processing

» Examination procedures include determining whether:

- there is a separate bank policy for merchant processing or whether it is incorporated within another bank policy, when the board approved the policy, when the policy for merchant processing was last updated, and whether the policy meets the criteria set forth in the guidance; and
- the board evaluates policies for changing market and business conditions at least annually, and whether the policies are in line with the overall strategic plan for this activity;
- the board has adopted a policy for underwriting new independent sales organizations or member service providers (ISOs/MSPs) that meets the criteria set forth in the guidance; and
- the board has reviewed the department's bonding needs.

» The board and management should limit the bank's volume of merchant processing relative to its capital, its risk profile, and management's ability to monitor and control the risks of merchant processing.

- The board-approved policy governing merchant processing should require at least an annual analysis of capital allocated for merchant processing activities, and the analysis should be approved by the board.
    - *Examination procedures include determining whether the board has established policies on concentration limits in relation to bank capital, earnings, or sales volumes as appropriate.*
- Any collateral obligations for the merchant processing activity should be reported to the board and management on a regular basis.
- Management and the board should be kept informed of the merchant processing department's profitability.

» The board and management should regularly receive reports that enable them to gauge the merchant processing department's risk.

- The level of detail and frequency of reporting to the board is contingent on the size and risk profile of the operation in relation to the overall operations of the bank and its capital base.
- For an acquiring bank, at a minimum, reports to the board of directors should include information for each portfolio segment, including agent bank and ISO/MSP portfolios. Information should include sales volumes, merchant types, profitability, charge-back activity, and fraud activity.

pp. Mortgage Banking

» The board of directors and senior management should outline the strategies and goals of their mortgage banking operation and should define the mortgage banking operation's permissible activities, lines of authority, operational responsibilities, and acceptable risk levels.

» The board and management should ensure that the internal audit staff has the necessary qualifications and expertise to review mortgage banking activities, including all related IT environments, or should mitigate voids with qualified external sources.

» The board and management should develop prudent risk management policies and procedures, including earnings-at-risk (EaR) or value-at-risk (VaR) parameters, to guard against adverse financial results.

qq. Oil and Gas Production Lending

» The bank's board of directors is responsible for ensuring control systems are in place to monitor compliance with established O&G lending policies.

- Bank management should provide the board of directors with an analysis of the risk posed by O&G lending activities as well as risks correlated to the O&G industry and their potential effect on the bank's asset quality, earnings, capital, and liquidity.
- The results should be an important consideration in a bank's allowance for loan and lease losses (ALLL) and capital and liquidity planning processes and should be taken into consideration as part of the board's action to approve risk limits as a percentage of total capital pertaining to O&G lending.
- The board should update and approve O&G policies annually.

» The OCC expects the board of directors to ensure that the bank maintains adequate capital relative to concentration risks, including concentrations pertaining to O&G related lending.

» Given that O&G lending decisions rely on quality engineering reports, the board should ensure that the size of the engineering staff is sufficient to enable timely completion of work so all borrowing base redeterminations can be promptly completed.

» The board should ensure that the O&G engineering function is independent of the O&G loan production and credit approval functions. While engineers may have communication with and input from loan production personnel to facilitate credit analysis, the reporting line for the engineering function should be separate from the production line.

rr. Other Real Estate Owned

» 12 C.F.R. 7.100(d) provides that, after holding real estate acquired for future expansion for one year, the bank must state, by resolution of the board of directors or an appropriately authorized bank official or subcommittee of the board, definite plans for the real estate's use.

» The board should adopt and annually review OREO policies that:

- Establish responsibilities and accountability.
- Require that risk management processes be established.
- Include written guidelines. If not, evaluate whether guidelines should be in writing, given the bank's complexity.

ss. Private Placements

» Examination procedures include determining whether the board has adopted written policies for private placements that:

- Define objectives.
- Provide guidelines for fee determinations based on: size of transaction; anticipated degree of difficulty or time involved; and payment of negotiated fees at various stages of the transaction.
- Require that bank officers act in an advisory rather than agent capacity in all negotiations.
- Recognize possible conflicts of interest, and establish appropriate procedures regarding: the purchase of bank-advised private placements with funds managed by the bank or an advisory affiliate; loans to investors to purchase private placements; use of proceeds of an

advised placement to repay the issuer's debts to the bank; and dealings with unsophisticated or non-institutional investors who have other business relationships with the bank.

- Require legal review of each placement prior to completion.
- Direct officers to obtain certified financial statements from the seller.
- Require distribution of certified financial statements to interested investors.
- Require officers to request a written statement of investment objectives or requirements from interested investors.
- Provide for a supervisory management review to determine if a placement is suitable for the investor.

tt. Rating Credit Risk

» The board of directors should approve the credit risk rating system and assign clear responsibility and accountability for the risk rating process. The board should receive sufficient information to oversee management's implementation of the process.

» The board and senior management must ensure that a suitable framework exists to identify, measure, monitor, and control credit risk. Board-approved policies and procedures should guide the risk rating process. These policies and procedures should establish the responsibilities of various departments and personnel. The board and management also must instill a credit culture that demands timely recognition of risk and has little tolerance for rating inaccuracy. Unless the board and senior management meet these responsibilities, their ability to oversee the loan portfolio can be severely hampered.

uu. Retail Lending Examination Procedures

» Examination procedures include determining whether the board has approved and annually reviewed consumer loan policies and whether the board or senior management has reviewed and approved the incentive pay program prior to implementation.

vv. Retail Nondeposit Investment Products

» A bank's board is ultimately responsible for the bank's provision of a retail nondeposit investment product ("RNDIP") sales program regardless if this business is conducted directly by the bank, by affiliated or unaffiliated third parties under a networking arrangement with the bank, or by some combination of these entities.

- The bank's board and bank management should implement effective program management over the RNDIP sales activities.
- The board establishes the risk appetite and strategic direction for a bank's RNDIP sales program.
  - *This includes finding the strategic fit for the RNDIP sales program within the bank's retail distribution channel and considering the bank's other asset management related business lines.*

» The board is responsible for providing the necessary managerial, financial, technological, and organizational resources to achieve the bank's strategic goals and objectives.

- This includes responsibility for the selection and retention of an experienced and competent management team responsible for supervising bank direct RNDIP sales activities and for overseeing the third parties used in the sales programs.
- The board may assign authority for the management of

the RNDIP sales program to bank officers, specific directors, employees, or committees.

» In carrying out its oversight responsibilities, a larger bank's board commonly designates a bank RNDIP oversight committee charged with risk identification, risk monitoring, and decision making within the board's established risk appetite.

- The RNDIP oversight committee should implement formalized governance that requires a charter; membership; identification of voting members, including members with veto power; quorums; frequency of meetings; and the maintenance of well-documented minutes to record decisions.

- A senior bank manager responsible for the bank's RNDIP sales program should lead the oversight committee. This committee should establish the necessary management information required to carry out its oversight responsibilities.

» The board of directors should adopt and periodically review the written program management statement. The expectation is that the written program management statement is reviewed and reaffirmed by the board or a board-designated committee at least annually or more frequently if warranted.

» A bank's board should approve the initial choice of a third party, such as securities broker-dealers, insurance agents, or registered investment advisors, that may provide RNDIPs through bank distribution channels and should approve the written agreement, also known as the networking agreement, between the bank and such third party.

- The board should ensure effective risk assessment and due diligence processes are implemented by senior management to properly oversee the third parties engaged in the bank's RNDIP sales program.

ww. Residential Real Estate Lending

» If the board and management decide to enter the subprime residential real estate ("RRE") lending or servicing business, they should establish policies and procedures as well as internal controls to identify, measure, monitor, and control the additional risks. The board should approve these policies annually.

» The board and management should carefully assess all risks associated with any proposed home equity conversion mortgage or proprietary reverse mortgage lending program and determine to what degree the risks are within the bank's articulated risk appetite.

» The board and management should set thresholds for effective resolution and actively address any situations that extend beyond the tolerances.

» The board should approve annually the bank's portfolio credit risk management process for home equity portfolios that is commensurate with its size, operational nature, and risk profile and should include compliance with regulatory real estate lending standards requiring lending policies that are consistent with safe and sound banking practices.

» The board and management should effectively limit the volume of loans and lines of credit subjected to risk-layering practices and avoid undue concentrations of layered risk in relation to regulatory capital and earnings.

» The board or designated committee is responsible for adopting and reviewing policies and procedures that establish an effective real estate appraisal and evaluation program.

» If an appraisal management company is used for any portion of the bank's program, the bank's board and management remain ultimately responsible and accountable for ensuring that any services performed

by a third party comply with all applicable laws and regulations, including that a bank and its agent must compensate fee appraisers at a rate that is customary and reasonable for appraisal services performed in the market area of the property being appraised.

» The board (or a board committee) and senior management are responsible for overseeing the bank's overall risk management processes, including the approval of private mortgage insurance provider contracts that involve critical activities. The board and management should ensure that the bank adheres to all loan underwriting, documentation, recording, collection, and record-keeping requirements of the private mortgage insurer so that the insurance remains in force.

» If a bank's RRE lending activities are of sufficient size and nature to warrant a quality control function, the board should ensure that the function is sufficiently independent of the loan production process to provide meaningful information about the quality of RRE lending activities.

» The board should require risk-based periodic audits and loan reviews of the bank's RRE lending activities. The board and management should ensure that the internal audit staff has the necessary qualifications and expertise to review RRE activities, including all related IT environments, or should mitigate voids with qualified external sources

xx. Retirement Plan Products and Services

» A bank's board is ultimately responsible for the bank's provision of retirement plan products and services (*see* 12 C.F.R. 9.4). The board must be kept adequately informed about risk identification and risk management in the bank retirement plan products and services line of business.

» The board, or its designated committee(s), must adopt policies that promote sound risk management processes, and should review the policies annually.

- These policies should provide management with guidance concerning the types of retirement plan products and services and level of risk acceptable to management.

- Senior management should ensure that the results of independent reviews of risk management processes with respect to third-party relationships are reported to the board.

yy. Risk Management of Financial Derivatives

» It is the responsibility of the board to hire a competent executive management team, endorse the corporate vision and the overall business strategy (including the institutional risk appetite), and hold executive management accountable for performance. This section of the Comptroller's Handbook further states that the board must understand the role derivatives play in the overall business strategy.

» The formality of board and senior management oversight mechanisms will differ depending on the derivatives activities conducted by the bank. However, the board and senior management must provide adequate resources (financial, technical expertise, and systems technology) to implement appropriate oversight mechanisms.

» On an ongoing basis, the board or appropriate committee should review and endorse significant changes in derivative activities. At least annually, the board, or a designated committee, should also approve key policy statements.

» Depending on the magnitude of the new product or activity and its impact on the bank's risk profile, senior

management, and in some cases, the board, should provide the final approval.

» This section of the Comptroller's Handbook notes that, although a bank's board of directors and senior management can readily approve policies delineating permissible derivative activities and risk tolerances, the volume and complexity of activities at many banks makes it impractical for these directors and senior management to oversee the day-to-day management of derivative activities. Consequently, they rely on strong risk control and audit functions to ensure compliance with policies.

» To ensure consistency between risk limits and business strategies, the board should annually approve risk limits as part of the overall budget process.

» The board and senior management should ensure that policies and procedures are established to address derivative transactions with affiliates. The policy should describe the nature of acceptable affiliate transactions, pricing, monitoring, and reporting.

» The board and management should evaluate price risk and interest rate risk for the bank as a whole, in addition to consideration of other risks.

» Regardless of the method for measuring and controlling interest rate risk, the board must be satisfied that effective controls are designed and implemented to limit the bank's vulnerability to interest rate risk.

» The board and senior management must institute a sound internal control framework to prevent losses caused by fraud and human error.

» The board of directors and senior management should ensure that the bank maintains sufficient capital to support the risks that may arise from its derivative activities. Significant changes in the size or scope of a bank's activities should prompt an analysis of the adequacy of the amount of capital supporting those activities. This analysis, which may be incorporated into the bank's periodic review of capital adequacy for all activities, should be approved by the board or senior management and be available for bank examiner review.

zz. Unique and Hard to Value Assets

» The bank's board of directors and senior management should take appropriate steps to identify, measure, control, and monitor the risks associated with investing and managing unique assets. The bank fiduciary has a duty to maintain and protect the value of a trust's assets and to make them productive.

» Board and management must commit to and support comprehensive risk management systems that effectively manage risk associated with unique assets. These systems should include specific processes for each class of unique assets held or managed by the bank's trust department.

B. FRB

1. Supervision and Regulation ("SR") Letters

a. SR 15-18: Federal Reserve Supervisory Assessment of Capital Planning and Positions for LISCC Firms and Large and Complex Firms/SR 15-19: Federal Reserve Supervisory Assessment of Capital Planning and Positions for Large and Noncomplex Firms

SR 15-18 applies to U.S. bank holding companies and intermediate holding companies of foreign banking organizations that are either: (i) subject to the FRB's Large Institution Supervision Coordinating Committee ("LISCC") framework or (ii) have total consolidated assets of $250 billion or more or consolidated total on-balance sheet foreign exposure of $10 billion or more.

SR 15-19 applies to U.S. bank holding companies and intermediate holding companies of foreign banking organizations that have

total consolidated assets of at least $50 billion but less than $250 billion, have consolidated total on-balance sheet foreign exposure of less than $10 billion, and are not LISCC firms.

» The FRB expects a firm to have sound governance over its capital planning process. In general, senior management should establish the capital planning process and the board of directors should review and periodically approve that process.

» An institution's board of directors is ultimately responsible and accountable for the institution's capital-related decisions and for capital planning. The institution's capital planning should be consistent with the strategy and risk appetite set by the board and with the firm's risk levels, including how risks at the firm may emerge and evolve under stress. The board must annually review and approve the firm's capital plan.

» The board should direct senior management to provide a briefing on their assessment of the firm's capital adequacy at least quarterly, and whenever economic, financial, or firm-specific conditions warrant a more frequent update.

- The briefing should describe whether current capital levels and planned capital distributions remain appropriate and consistent with capital goals. In their briefing, senior management should also highlight for the board any problem areas related to capital planning identified by senior management, internal audit, or supervisors.

» The board should hold senior management accountable for providing sufficient information on the firm's material risks and exposures to inform board decisions on capital adequacy and actions, including capital distributions. Information provided to the board should be clear, accurate, and timely. The board should direct senior management to provide this information at least quarterly and whenever economic, financial, or firm-specific conditions warrant a more frequent update. The information presented to the board should include consideration of a number of factors, such as:

- Macro-economic conditions and relevant market events;
- Current capital levels relative to budgets and forecasts;
- Post-stress capital goals and targeted real time capital levels (*see* section III.D of the guidance, "Capital Policy");
- Enterprise-wide and line-of-business performance;
- Expectations from stakeholders (including shareholders, regulators, investors, lenders, counterparties, and rating agencies);
- Potential sources of stress to the firm's operating performance; and
- Risks that may emerge only under stressful conditions.

» After receiving the information, the board should be in a position to understand the major drivers of the firm's projections under a range of conditions, including baseline and stress scenarios.

» The board should direct senior management to provide information about the firm's estimation approaches, model overlays, and assessments of model performance. The board should also receive information about uncertainties around projections of capital needs or limitations within the firm's capital planning process to understand the impact of these weaknesses on the process.

- This information should include key assumptions and the analysis of sensitivity of a firm's projections to changes in the assumptions.
- The board should incorporate uncertainties in projections and limitations in the firm's capital planning process into its decisions on capital adequacy and capital actions. It should also review and approve mitigating

steps to address capital planning process weaknesses.

» The board should direct senior management to establish sound controls for the entire capital planning process. The board should approve policies related to capital planning, and review them annually. The board should also approve capital planning activities and strategies. The board of directors should maintain an accurate record of its meetings pertaining to the firm's capital planning process.

» Material model overlays—either in isolation or in combination—should receive a heightened level of support and scrutiny, up to and including review by the firm's board of directors (or a designated committee), in instances where the impact on pro forma results is material.

» An institution should ensure that the key sensitivities are presented to senior management and the board in advance of decision-making around the firm's capital plan and capital actions. Sensitivity analysis should also be used to inform senior management, and, as appropriate, the board of directors about the potential uncertainty associated with models employed of the firm's projections under stress.

» On an annual basis, the internal audit function should report to senior management and the board of directors on the capital planning process to inform recommendations and decisions on the firm's capital plan.

- In addition, for firms subject to SR 15-18, a firm's internal audit function should brief the board of directors (or a designated committee thereof) and senior management at least quarterly on the status of key findings relating to the capital planning process.

- All deficiencies, limitations, weaknesses and uncertainties identified by the internal audit function that relate to the firm's capital planning process should be reported to senior management, and material deficiencies should be reported to the board of directors (or the audit committee of the board) in a timely manner.

» The capital policy should also specify the analysis and metrics that senior management and the board use to make capital distribution decisions. The capital policy should require that aggregated results be directly compared against the firm's stated post-stress capital goals, and that those comparisons are included within the standard reporting to senior management and the board of directors.

- A firm subject to SR 15-18 should include in its capital policy threshold levels for payout ratios that trigger management action; such action should include escalation to the board and potential suspension of capital distributions.

» A firm's capital contingency plan should reflect strategies for identifying and addressing potential capital shortfalls and specify circumstances under which the board of directors and senior management will revisit planned capital actions or otherwise institute contingency measures.

b. SR 15-15: Supervisory Concerns Related to Shareholder Protection Arrangements

» Examples of shareholder protection arrangements that have raised supervisory issues include (among others) provisions whereby the holding company's board of directors has the authority to nullify share purchases under certain circumstances, require the holding company to repurchase the shares of the company from a new owner of the shares, or take other actions that would significantly inhibit secondary market transactions in the shares of the holding company.

- These arrangements could include complete prohibitions on share transfers, as well as certain forms of buy-sell agreements, rights of first refusal, or similar arrange-

ments that sufficiently restrict the transfer of shares as to effectively prohibit most, if not all, transfers.

» The FRB may direct a holding company's board of directors to modify or remove a shareholder protection arrangement that gives rise to safety-and-soundness concerns.

- The corrective actions, if any, will vary depending on the facts and circumstances of the holding company, as well as applicable state and federal laws and regulations, corporate charter and by-laws, and other considerations.

c. SR 14-08: Consolidated Recovery Planning for Certain Large Domestic Bank Holding Companies (applies to eight domestic BHCs)

» Successful integration of recovery planning into existing firm processes should result in, among other things, timely escalation by management of identified weaknesses and planned responses to the firm's board of directors.

» The board should oversee the firm's recovery planning process. The board, or a designated committee thereof, should focus this oversight on the firm's ability to effectively identify and implement recovery options and oversee management's remediation of weaknesses identified in the firm's processes.

» A firm's recovery plan should describe the triggers that indicate when a firm enters recovery along with related escalation procedures for senior management action and notification of board of directors.

d. SR 14-03: Supervisory Guidance on DFA Company-Run Stress Testing for Banking Organizations with Total Consolidated Assets of More than $10 Billion but Less than $50 Billion

» With respect to DFA stress testing, the board of directors should ensure it remains informed about critical review of elements of the DFA stress tests, especially regarding key assumptions, uncertainties, and limitations.

» In addition, the board of directors and senior management of a $10-50 billion company must consider the role of stress testing results in normal business, including in the company's capital planning, assessment of capital adequacy, and risk management practices.

e. SR 13-24: Managing Foreign Exchange Settlement Risks for Physically Settled Transactions

» Applies only to institutions with $50 billion or more in total consolidated assets or institutions that engage in significant FX activities.

» The board of directors of a covered institution should oversee the management of the compliance function associated with settling foreign exchange transactions.

- Senior management should routinely communicate significant compliance matters to the board of directors.
- The board of directors may choose to delegate regular oversight to a single board member or a committee of the board.

f. SR 13-19: Guidance on Managing Outsourcing Risk

» The use of service providers does not relieve a financial institution's board of directors and senior management of their responsibility to ensure that outsourced activities are conducted in a safe-and-sound manner and in compliance with applicable laws and regulations. Policies governing the use of service providers should be established and approved by the board of directors, or an executive committee of the board. These policies

should establish a service provider risk management program that addresses risk assessments and due diligence, standards for contract provisions and considerations, ongoing monitoring of service providers, and business continuity and contingency planning.

» Senior management is responsible for regularly reporting to the board of directors on adherence to policies governing outsourcing arrangements.

» Service providers may want to contractually limit their liability. The board of directors and senior management of a financial institution should determine whether the proposed limitations are reasonable when compared to the risks to the institution if a service provider fails to perform.

g. SR 13-13: Supervisory Considerations for the Communication of Supervisory Findings

» While the board itself may not directly undertake the work to remediate supervisory findings as senior management is responsible for the organization's day-to-day operations, it is nevertheless important that the board be made aware of significant supervisory issues and ultimately be accountable for the safety and soundness and assurance of compliance with applicable laws and regulations of the organization.

» Depending upon the size and complexity of the organization, supervisory findings are communicated in writing through formal examination or inspection reports, reports summarizing the results of targeted reviews, a roll-up of those reviews into a comprehensive report, any other supervisory communication, or some combination thereof. These written communications (referred to collectively as "reports" in this document) are generally directed to the board of directors, or an executive-level committee of the board, as appropriate. In turn, the board of directors (or executive-level committee of the board) typically will direct the organization's management to take corrective action and will provide management with appropriate oversight, including approvals of proposed management actions as necessary.

» Following its review of the report, the banking organization's board of directors is required to provide a written response to the Reserve Bank regarding its plan, progress, and resolution of the MRA.

» Following its review of MRIAs discussed in the report, the banking organization's board of directors is required to respond to the Reserve Bank in writing regarding corrective action taken or planned along with a commitment to corresponding timeframes.

h. SR 13-1: Supplemental Policy Statement on the Internet Audit Function and its Outsourcing

» This guidance applies to state member banks, domestic bank and savings and loan holding companies, and U.S. operations of foreign banking organizations with total consolidated assets of $10 billion or more.

» The internal audit charter, which describes the purpose, authority, and responsibility of the internal audit function, should be approved by the audit committee of the institution's board of directors.

» Internal audit should understand risks faced by the institution and confirm that the board of directors and senior management are actively involved in setting and monitoring compliance with the institution's risk tolerance limits.

» The board of directors and senior management are responsible for ensuring that the institution has an effective system of internal controls. As indicated in the 2003 Interagency Policy Statement on the Internal Audit Function and its Outsourcing, this responsibility cannot be delegated to others within the institution or to ex-

ternal parties. Further, the board of directors and senior management are responsible for ensuring that internal controls are operating effectively.

» Information supplied by an internal audit vendor should provide the board of directors, its audit committee, and senior management with an accurate report on the control environment, including any changes necessary to enhance controls.

i. SR 12-17: Consolidated Supervision Framework for Large Financial Institutions

» This guidance applies to firms subject to the FRB's LISCC framework, domestic bank and savings and loan holding companies with consolidated assets of $50 billion or more, and large foreign banking organizations with combined assets of U.S. operations of $50 billion or more.

» To support effective capital and liquidity planning, and the adequacy of capital and liquidity positions, each firm should establish goals for capital and liquidity positions that are approved by the firm's board of directors and reflect the potential impact of legal or regulatory restrictions on the transfer of capital or liquidity between legal entities.

» In order for a firm to be sustainable under a broad range of economic, operational, legal or other stresses, its board of directors (or equivalent for the U.S. operations of FBOs) should provide effective corporate governance with the support of senior management. The board is expected to establish and maintain the firm's culture, incentives, structure, and processes that promote its compliance with laws, regulations, and supervisory guidance. Each firm's board of directors and committees, with support from senior management, should:

- Maintain a clearly articulated corporate strategy and institutional risk appetite. The board should set direction and oversight for revenue and profit generation, risk management and control functions, and other areas essential to sustaining the consolidated organization.
- Ensure that the firm's senior management has the expertise and level of involvement required to manage the firm's core business lines, critical operations, banking offices, and other material entities. These areas should receive sufficient operational support to remain in a safe and sound condition under a broad range of stressed conditions.
- Maintain a corporate culture that emphasizes the importance of compliance with laws and regulations and consumer protection, as well as the avoidance of conflicts of interest and the management of reputational and legal risks.
- Ensure the organization's internal audit, corporate compliance, and risk management and internal control functions are effective and independent, with demonstrated influence over business-line decision making that is not marginalized by a focus on short-term revenue generation over longer-term sustainability.
- Assign senior managers with the responsibility for ensuring that investments across business lines and operations align with corporate strategies, and that compensation arrangements and other incentives are consistent with the corporate culture and institutional risk appetite.
- Ensure that management information systems (MIS) support the responsibilities of the board of directors to oversee the firm's core business lines, critical operations, and other core areas of supervisory focus.

» Each firm should ensure that recovery planning is sufficiently integrated into corporate governance structures and processes, subject to independent validation, and effectively supported by related MIS reporting to the board and its committees.

» For firms required to submit a resolution plan to the FRB and FDIC, the FRB and the FDIC jointly review the resolution plan relative to supervisory requirements, including an analysis of whether resolution planning is sufficiently integrated into corporate governance structures and processes, subject to independent validation, and effectively supported by related MIS reporting to the board of directors and its committees.

j. SR 12-4: Upgrades of Supervisory Ratings for Banking Organizations with $10 Billion or Less in Total Consolidated Assets

» When assessing whether a rating upgrade is warranted, the FRB will evaluate the strength of core financial components, overall risk management, and board of directors' oversight. Specific considerations include (among others):

- the extent to which the board provides strategic review and oversight of the banking organization's core financial factors and risk management and actively engages in the process of correcting deficiencies; and
- management's projections and assumptions related to core financial factors are reasonable and subject to regular board review and oversight.

k. SR 11-7: Guidance on Model Risk Management

» *See* description in corresponding OCC Bulletin 2011-12 described above.

l. SR 10-17: Underwriting Standards for Small Business Loans Originated under the Small Business Lending Fund Program

» *See* Interagency Guidance on Underwriting Standards for Small Business Loans Originated Under the Small Business Lending Fund Program described below.

m. SR 09-4: Applying Supervisory Guidance and Regulations on the Payment of Dividends, Stock Redemptions, and Stock Repurchases at BHCs

» A BHC's board of directors should take into account the following factors when considering the payments of dividends, stock redemptions, or stock repurchases:

- Overall asset quality, potential need to increase reserves and write down assets, and concentrations of credit;
- Potential for unanticipated losses and declines in asset values;
- Implicit and explicit liquidity and credit commitments, including off-balance sheet and contingent liabilities;
- Quality and level of current and prospective earnings, including earnings capacity under a number of plausible economic scenarios;
- Current and prospective cash flow and liquidity;
- Ability to serve as an ongoing source of financial and managerial strength to insured depository institution subsidiaries, including the extent of double leverage and the condition of subsidiary depository institutions;
- Other risks that affect the BHC's financial condition and are not fully captured in regulatory capital calculations;
- Level, composition, and quality of capital; and
- Ability to raise additional equity capital in prevailing market and economic conditions.

» When a BHC's board of directors is deciding on the level of dividends to declare, it should consider, among other things, the factors discussed above. It is particularly important for a banking organization's board of directors to ensure that the dividend level is prudent relative to the organization's financial position and is not based on overly optimistic earnings scenarios.

- Moreover, because the period between declaration of a dividend and the payment date may be as much as 60 days, in making a declaration, the board of directors should consider any potential events that may occur before the payment date that could affect its ability to pay while still maintaining a strong financial position.

» While many organizations place great importance on consistently paying dividends, a board of directors should strongly consider, after careful analysis of the factors described above, reducing, deferring, or eliminating dividends when the quantity and quality of the BHC's earnings have declined or the BHC is experiencing other financial problems, or when the macroeconomic outlook for the BHC's primary profit centers has deteriorated. As a general matter, the board of directors of a BHC should inform the FRB and should eliminate, defer, or significantly reduce the BHC's dividends if:

- The BHC's net income available to shareholders for the past four quarters, net of dividends previously paid during that period, is not sufficient to fully fund the dividends;

- The BHC's prospective rate of earnings retention is not consistent with the BHC's capital needs and overall current and prospective financial condition; or

- The BHC will not meet, or is in danger of not meeting, its minimum regulatory capital adequacy ratios.

n. SR 08-09: Consolidated Supervision of Domestic BHCs and the Combined US Operations of FBOs

» With respect to U.S. BHCs with $10 billion or more in total assets, the board and its committees should have an ongoing understanding of key inherent risks, associated trends, primary control functions, and senior management capabilities. Primary expectations for the board and its committees include:

- Selecting competent senior managers, ensuring that they have the proper incentives to operate the organization in a safe and sound manner, and regularly evaluating senior managers' performance;

- Establishing, communicating, and monitoring (for example, by reviewing comprehensive MIS reports produced by senior management) institutional risk tolerances and a corporate culture that emphasizes the importance of compliance with the law and ethical business practices;

- Approving significant strategies and policies;

- Demonstrating leadership, expertise, and effectiveness;

- Ensuring the organization has an effective and independent internal audit function;

- Ensuring the organization has appropriate policies governing the segregation of duties and avoiding conflicts of interest; and

- Ensuring that public disclosures (i) are consistent with how the board and senior management assess and manage the risks of the organization, (ii) balance quantitative and qualitative information with clear discussions about risk management processes, and (iii) reflect evolving disclosure practices for peer organizations.

o. SR 08-08: Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles

» Boards of directors are responsible for setting an appropriate culture of compliance within their organizations, for establishing clear policies regarding the management of key risks, and for ensuring that these policies are adhered to in practice.

- The board should have an appropriate understanding of the types of compliance risks to which the organization is exposed.
  - *The level of technical knowledge required of directors to fulfill these responsibilities may vary depending on the particular circumstances at the organization.*
- The board should ensure that senior management is fully capable, qualified, and properly motivated to manage the compliance risks arising from the organization's business activities in a manner that is consistent with the board's expectations.
- The board should ensure that its views about the importance of compliance are understood and communicated by senior management across, and at all levels of, the organization through ongoing training and other means.
- The board should ensure that senior management has established appropriate incentives to integrate compliance objectives into the management goals and compensation structure across the organization, and that appropriate disciplinary actions and other measures are taken when serious compliance failures are identified.
- Finally, the board should ensure that the corporate compliance function has an appropriately prominent status within the organization.

» The board should be knowledgeable about the general content of the compliance program and exercise appropriate oversight of the program.

- Accordingly, the board should review and approve key elements of the organization's compliance risk management program and oversight framework, including firmwide compliance policies, compliance risk management standards, and roles and responsibilities of committees and functions with compliance oversight responsibilities.
- The board should oversee management's implementation of the compliance program and the appropriate and timely resolution of compliance issues by senior management.
- The board should exercise reasonable due diligence to ensure that the compliance program remains effective by at least annually reviewing a report on the effectiveness of the program.
- The board may delegate these tasks to an appropriate board-level committee.

p. SR 04-18: Bank Holding Company Rating System (12/6/2004)

» Risk management component.

- To receive a rating of 1 (strong), the board and management need to be forward-looking and active participants in managing risk. Management ensures that appropriate policies and limits exist and are understood, reviewed, and approved by the board.
- To receive a rating of 2 (satisfactory), board and senior management oversight, policies and limits, risk monitoring procedures, reports, and management information systems need to be considered satisfactory and effective in maintaining a safe and sound institution.

» Risk management subcomponents: board and senior management oversight.

- A rating of 1 (strong) signifies that the board and senior management are forward-looking, fully understand the types of risk inherent in the BHC's activities, and actively participate in managing those risks. The board is expected to approve overall business strategies and significant policies, and ensure that senior management is fully capable of managing the activities that the BHC conducts.
- Rating 2 (satisfactory) indicates that board and senior management have an adequate understanding of the organization's risk profile and provide largely effective oversight of risk management practices. In this regard, the board is expected to approve all major business strategies and significant policies, and ensure that senior management is capable of managing the activities that the BHC conducts.

q. SR 01-13: Supervisory Guidance Relating to a Change to Permissible Securities Activities of State Member Banks (5/14/2001)

» Senior management and the board of directors should establish credit quality and position risk guidelines, including concentration risk.

r. SR 99-7: Supervisory Guidance Regarding the Investment of Fiduciary Assets in Mutual Funds and Potential Conflicts of Interest (3/26/1999)

» The institution should establish written policies and procedures governing the acceptance of fees or other compensation from mutual fund providers as well as the use of proprietary mutual funds. The policies must be reviewed and approved by the institution's board of directors or its designated committee.

s. SR 98-18: Lending Standards for Commercial Loans (6/23/1998)

» Bank directors and senior managers have the obligation to monitor lending practices and to ensure that their policies are enforced and that lending practices more generally remain within the overall ability of the institution to manage.

t. SR 98-9: Assessment of Information Technology in the Risk-Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations (4/20/1998)

» An organization's management and board of directors are expected to manage effectively the risks associated with information technology.

» The board of directors and senior management are expected to adequately identify, measure, monitor, and control the significant risks associated with information technology for the overall organization and its major business activities.

u. SR 97-25: Risk-Focused Framework for the Supervision of Community Banks (10/1/1997) / SR 95-51: Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies (11/14/1995)

» The board and executive management are expected to have the required knowledge, experience, and training to perform their duties.

» The board is expected to:

- have a management succession plan, either formally or informally;

- use an effective planning process and implements dynamic strategies;
- establish control activities encompassing policies and implementation procedures that ensure management's directives are achieved;
- establish an effective audit program;
- minimize operating management's ability to override policies and procedures through effective monitoring and enforcement of established guidelines;
- establish adequate lending policies, procedures, and operating strategies; and
- approve a list of appraisers as part of the loan or appraisal policy.

» If the bank has chosen not to obtain an external audit, the board of directors should document its reasons including whether the auditing program provides sufficient coverage of areas of potential concern or unique risk.

v. SR 97-24: Risk-Focused Framework for Supervision of Large Complex Institutions (10/27/1997)

» Boards of directors have ultimate responsibility for the level of risk taken by their institutions. Accordingly, they should approve the overall business strategies and significant policies of their organizations, including those related to managing and taking risks, and should also ensure that senior management is fully capable of managing the activities that their institutions conduct.

» In assessing the quality of the oversight by boards of directors and senior management, examiners should consider whether the institution follows policies and practices such as those described below:

- The board and senior management have identified and have a clear understanding and working knowledge of the types of risks inherent in the institution's activities and make appropriate efforts to remain informed about these risks as financial markets, risk management practices, and the institution's activities evolve.
- The board has reviewed and approved appropriate policies to limit risks inherent in the institution's lending, investing, trading, trust, fiduciary and other significant activities or products.
- The board and management are sufficiently familiar with and are using adequate record keeping and reporting systems to measure and monitor the major sources of risk to the organization.
- The board periodically reviews and approves risk exposure limits to conform with any changes in the institution's strategies, addresses new products, and reacts to changes in market conditions.

» The institution's audit committee or board of directors is expected to review the effectiveness of internal audits and other control review activities on a regular basis.

w. SR 97-21: Risk Management and Capital Adequacy of Exposures Arising from Secondary Market Credit Activities (7/11/1997)

» Both the board of directors and senior management are responsible for ensuring that they fully understand the degree to which the organization is exposed to the credit, market, liquidity, operational, legal, and reputational risks involved in the institution's secondary market credit activities.

- They are also responsible for ensuring that the formality and sophistication of the techniques used to manage

these risks are commensurate with the level of the organization's activities.

» The board should approve all significant polices relating to the management of risk arising from secondary market credit activities and should ensure that the risk exposures are fully incorporated in board reports and risk management reviews.

x. SR 96-38: Uniform Financial Institutions Rating System (12/27/1996)

» Generally, directors need not be actively involved in day-to-day operations; however, they must provide clear guidance regarding acceptable risk exposure levels and ensure that appropriate policies, procedures, and practices have been established.

y. SR 96-10: Risk-Focused Fiduciary Examinations (4/24/1996)

» The boards of directors should approve overall fiduciary business strategies and policies including those related to identifying, measuring, monitoring and controlling fiduciary risks.

» The boards of directors must understand the nature of the risks significant to their organization and ensure that management is taking the steps necessary to manage these risks.

» An institution's directors and senior management should establish fiduciary and fiduciary risk management policies and procedures commensurate with the types of activities the institution conducts.

» The board of directors and/or the audit committee is expected to review the effectiveness of internal audits and other control review activities on a regular basis.

z. SR 94-53: Investment Adviser Activities (10/25/1994)

» All major policies and procedures pertaining to advisory activities should be reviewed periodically and approved by the organizations' boards of directors.

» The holding company's senior management and its board of directors are expected to have policies and procedures in place to monitor the activities of investment adviser subsidiaries to ensure that the risks associated with the conduct of this activity are not in conflict with the parent company's overall risk tolerance parameters.

aa. SR 93-69: Examining Risk Management and Internal Controls for Trading Activities of Banking Organizations (12/20/1993)

» The board of directors should approve all significant policies relating to the management of risks throughout the institution.

» The board should be informed regularly of the risk exposure of the institution and should regularly re-evaluate significant risk management policies and procedures with special emphasis placed on those defining the institution's risk tolerance regarding these activities.

» The board of directors should also conduct and encourage discussions between its members and senior management, as well as between senior management and others in the institution, regarding the institution's risk management process and risk exposure.

» Legal risks should be limited and managed through policies developed by the institution's legal counsel (typically in consultation with officers in the risk management process) that have been approved by the bank's senior management and board of directors.

bb. SR 93-36: Preliminary Examiner Guidelines for Regulation F – Interbank Liabilities (6/18/1993)

» Policies and procedures addressing exposures to correspondents must be reviewed annually by the bank's board of directors, but individual correspondent relationships need not be approved by the board.

» A bank may rely on another party, such as a bank rating agency or the bank's holding company, to assess the financial condition of or select a correspondent, provided that the bank's board of directors has reviewed and approved the general assessment or selection criteria used by that party.

cc. SR 93-1: Real Estate Lending Standards (1/11/1993)

» The institution's board of directors must review and approve at least annually its real estate lending policies.

» The board of directors is responsible for establishing standards for the review and approval of exception loans.

dd. SR 91-4: Guidelines for the Inspection of Investment Adviser Subsidiaries of Bank Holding Companies

» The board is expected to adequately seek to assure the integrity of the institution's records and operational systems through adoption of formal policies and provisions for auditing.

» The institution's board or a board committee is expected to consider, periodically review, and provide for insurance protection.

» The board is expected to define and approve the institution's general investment standards, review and selection responsibilities.

» Where volume of activity warrants, the allocation of brokerage business should be controlled through an approved list which is periodically reviewed and approved by the institution's board or a senior officer level committee.

2. Bank Holding Company Supervision Manual

(References are to Manual Section Numbers)

The Foreword to the Bank Holding Company Supervision Manual states that it "has been prepared by Federal Reserve supervision personnel to provide guidance to examiners as they conduct on-site inspections of bank holding companies (BHCs) and their non-bank subsidiaries." Section 1030 (Use of the Manual) further states that "[e]xaminers may exercise a measure of discretion depending upon the characteristics of the organization under inspection."

a. Supervision of Subsidiaries

» Holding company inspection objectives include determining the following: (1) whether the board of directors of the parent company is cognizant of and performing its responsibilities; (2) the adequacy of written policies and compliance with such policies by the parent and its subsidiaries; (3) whether the board is properly informed as to the financial conditions, trends and policies of its subsidiaries; and (4) the level of supervision over subsidiaries and whether the supervision as structured has a beneficial or detrimental effect upon the subsidiaries. 2010.0.3.

» Holding company inspection procedures include (1) determining whether the board of directors of the parent company reviews the audit reports, regulatory examination reports, and board minutes of its subsidiaries, and (2) reviewing the minutes of the board and executive committees of the parent to determine whether the parent company reviews loan delinquency reports, comparative balance sheets and comparative income statements of the subsidiaries. 2010.0.4.

b. Loan Administration and Lending

» The board of directors must review and approve the institution's lending policies at least annually. 2010.2.1.

» The lending decision for commercial loans is properly that of boards of directors and senior management of banking institutions, and not of their supervisory agencies. However, in fulfilling their roles, directors and senior managers have the obligation to monitor lending practices and to ensure that their policies are enforced and that lending practices generally remain within the overall ability of the institution to manage. 2010.2.2.

» The institution's designated risk appetite should be supported by an analysis of the potential effect on earnings, capital, liquidity, and other risks that result from these positions, and should be approved by its board of directors. 2010.2.3.1.3.

» The board of directors and management should establish clear expectations for the disposition of pipeline transactions that are not sold according to their original distribution plan. 2010.2.3.1.7.

» Higher-risk credits, including leveraged-finance transactions, require frequent monitoring by banking organizations. At least quarterly, management and the board of directors should receive comprehensive reports about the characteristics and trends in such exposures. 2010.2.3.1.1.8.

» Examiners should determine whether an institution's board of directors and management have established policies for leveraged finance that minimize the risks posed by potential legal issues and conflicts of interest. 2010.2.3.1.4.

» Banking organizations should accurately track the volume of HLTV loans, including HLTV home equity and residential mortgages, and report the aggregate of such loans to the banking organization's board of directors. 2010.2.4.7.5.

» Examination procedures include (a) a determination of whether the information provided to the directorate and senior management is sufficient for them to make judgments about the quality of the portfolio and to determine appropriate corrective action, (b) an evaluation of the effectiveness of the holding company's self-monitoring of adherence to loan policy, and (c) a discussion of matters of concern with the senior management and the board of directors of the bank holding company. 2010.2.5.

c. Consolidated Planning Process

» In supervising subsidiaries, a holding company is advised of the importance of integrating subsidiaries into a consolidated plan. In this respect, the planning process should be formalized and include a long-range focus, intermediate term objectives, and budgets that are written and adopted by the parent's board of directors. The long-range goals, intermediate term objectives and short-term goals should be periodically reviewed, preferably annually, by the holding company's board of directors. 2010.4.

» Inspection objectives include determining if the board of directors of the parent holding company is making judgments and decisions based on adequate information flowing from the management and financial reporting systems of the organization. 2010.4.1

» Inspection procedures include an evaluation of the participation by the board of directors of the parent in giving overall direction to the organization, and a determination of the degree of control exercised by the parent company over the entire organization. 2010.4.2.

d. Financial Institution Subsidiary Retail Sales of Nondeposit Investment Products

» The Interagency Policy Statement on the Retail Sale of Non-deposit Investment Products (described below)

does not directly apply to bank holding companies; however, the board of directors of holding companies should consider and administer the provisions of the statement with regard to the holding company's supervision of its banking subsidiaries that offer such products to retail customers. 2010.6.

e. Fees Involving Investments of Fiduciary Assets in Mutual Funds and Potential Conflicts of Interest

» *See* SR 99-7: Supervisory Guidance Regarding the Investment of Fiduciary Assets in Mutual Funds and Potential Conflicts of Interest, above. 2010.12.1.

f. Split-Dollar Life Insurance

» For bank holding companies that have a split-dollar life insurance arrangement with a subsidiary, inspection procedures include determining whether the parent company's board of directors has established policies and implemented procedures for transactions between the insurance carrier and the parent company to prevent unauthorized borrowing or cancellation of any insurance policy that has a cash surrender value. 2020.9.

g. Management Information Systems

(1) POLICY STATEMENT ON THE INTERNAL AUDIT FUNCTION AND ITS OUTSOURCING

» *See* Interagency Policy Statement on the Internal Audit Function and its Outsourcing and the Supplemental Interagency Policy Statement on the Internal Audit Function and its Outsourcing described below. 2060.05.1.1.

(2) AUDIT

» When an independent auditor is used, an institution's board of directors must select an external auditor that will satisfy the independence requirements of the AICPA and the relevant requirements and interpretations of the SEC. 2060.05.2. FRB inspection procedures include determining whether an audit program is annually reviewed and approved by the board of directors. 2060.1.4.

» FRB examination objectives include determinations as to whether (a) the internal audit function and the internal audit outsourcing arrangement of the parent company and its subsidiaries are adequately managed by the board of directors and senior management (2060.05.3), and (b) audit reports are submitted on a timely basis to the directors and senior management (2060.1.4); examiners should review the engagement letter between the board of directors and the outside auditor. 2060.1.4.

(3) INSURANCE

» Once appropriate insurance coverage has been acquired, procedures should be established for the periodic review of the program to assure the continuing adequacy of the coverage. Particularly for large bank holding companies, these procedures should include at least an annual review of the program by the board of directors of the parent organization. 2060.5.1.

» Inspection procedures include reviewing the manner and frequency of presentations to the board of directors of the insurance coverage. 2060.5.8.

h. Maintenance of an Appropriate Allowance for Loan and Lease Losses

» It is the responsibility of the board of directors and management of each institution to maintain the ALLL at an adequate level. 2065.3.1.2.1.

» As part of the ALLL maintenance efforts, an institution's

loan review program should provide for at least annual reports to the board of directors. 2065.3.1.5.1.

» The loan review function should report directly to the board of directors. The board of directors should approve the scope of loan reviews at least annually. A report that summarizes the result of the loan review should be submitted to the board of directors on at least a quarterly basis. The board of directors should be informed more frequently than quarterly when material adverse trends are noticed. 2065.3.1.5.2.

i. ALLL Methodologies and Documentation

» Amounts reported periodically for the provision of loan and lease losses and the ALLL should be reviewed and approved by the board of directors. To ensure the methodology remains appropriate for the institution, the board of directors should have the methodology periodically validated and, if appropriate, revised. Further, the audit committee should oversee and monitor the internal controls over the ALLL-determination process. 2065.4.1

» To verify that ALLL balances are presented fairly in accordance with GAAP and are auditable, management should prepare a document that summarizes the amount to be reported in the financial statements for the ALLL. The board of directors should review and approve this summary. 2065.4.1.6.

j. Risk-Focused Safety and Soundness Inspections

» Regardless of the approach, the types and levels of risk an institution is willing to accept should reflect the risk appetite determined by its board of directors. 2124.01.61.

» Management must report at least annually to the board of directors or an appropriate board committee regarding customer information security. Such reports should describe the overall status of the information security program and the bank holding company's compliance with applicable regulatory guidelines. 2124.4.

k. Trading Activities of Banking Organizations (Risk Management and Internal Controls)

» The board of directors, senior-level management, and members of independent risk management functions are all important participants in the risk management process. Examiners should ensure that these participants are aware of their responsibilities and that they adequately perform their appropriate role in managing the risk of trading and derivative activities. 2125.0.1.

» The board of directors should approve all significant policies relating to the management of risks throughout the organization. 2125.0.1.1.

» The board should be informed regularly of risk exposure and should regularly reevaluate significant risk management policies and procedures with special emphasis placed on those defining the institution's risk tolerance regarding these activities. 2125.0.1.1.

- The board of directors should also conduct and encourage discussions between its members and senior management, as well as between senior management and others in the organization, regarding its risk management process and risk exposure.

l. Model Risk Management

» Model risk governance is provided at the highest level by the board of directors and senior management when they establish a bank-wide approach to model risk management. As part of their overall responsibilities, a bank's board and senior management should establish a strong model risk-management framework that fits into

the broader risk management of the organization. That framework should be grounded in an understanding of model risk—not just for individual models but also in the aggregate. The framework should include standards for model development, implementation, use, and validation. 2126.0.6.1.

- While the board is ultimately responsible, it generally delegates to senior management the responsibility for executing and maintaining an effective model risk-management framework.

- Board members should ensure that the level of model risk is within their tolerance and should direct changes where appropriate. These actions will set the tone for the whole organization about the importance of model risk and the need for active model risk management.

m. Investment Securities and End-User Derivatives Activities

» *See* FFIEC Supervisory Policy Statement on Investment Securities and End-User Derivatives Activities described below. 2126.1.1.4-5.

n. Structured Notes

(1) ASSET SECURITIZATIONS

» With respect to asset securitizations, a bank holding company's board of directors and management are expected to develop and implement policies that limit the amount of residual interests that may be carried as a percentage of total equity capital. 2128.02.8.

» Inspection objectives with respect to securitization activities include a determination that major policies and procedures, including internal credit-review and -approval procedures and "in house" exposure limits are reviewed periodically and approved by the bank holding company's board of directors. 2128.02.10.

(2) CREDIT-SUPPORTED AND ASSET-BACKED COMMERCIAL PAPER

» A banking organization such as a bank holding company participating in an asset-backed commercial paper program should ensure that such participation is clearly and logically integrated into its overall strategic objectives. Significant policies and procedures should be approved and reviewed periodically by the organization's board of directors. 2128.03.4.

(3) SECURITIZATION COVENANTS LINKED TO SUPERVISORY ACTIONS OR THRESHOLDS

» The board and management should ensure that covenants relating to supervisory actions or thresholds are not included in securitization documents. 2128.05.

(4) VALUATION OF RETAINED INTERESTS AND RISK MANAGEMENT OF SECURITIZATION ACTIVITIES

» The board of directors and management are expected to develop and implement policies that limit the amount of retained interests that may be carried as a percentage of total equity capital, based on the results of their valuation and modeling processes. 2128.06.10.

o. Credit Derivatives – Risk and Capital Adequacy Management of the Exposures Arising from Secondary-Market Credit Activities

» The board of directors should approve all significant policies relating to the management or risk arising from secondary-market credit activities and should ensure that the risk exposures are fully incorporated in board reports and risk-management reviews. 2129.05.4.1.

p. Futures, Forward and Option Contracts

» Inspection objectives with respect to an institution's futures, forward and option contract activities include:

- ascertaining whether the banking organization's board of directors has established written limitations with respect to financial-contract positions (Note: The bank holding company policy statement (at 12 C.F.R. 225.142, described above) requires that the board of directors establish written policies and position limitations in connection with financial-contract activities. If a committee has been delegated similar responsibilities within the organization, and a committee makes the decision, its recommendation should be ratified by the board of directors.).

- determining whether the board of directors, a duly authorized committee thereof, or internal auditors review at least monthly financial-contract positions to ascertain compliance with limitations. 2130.0.13.

q. Support of Bank-Affiliated Investment Funds

» In the limited instances when a bank provides financial support to affiliate-advised investment funds, the bank's procedures should include an oversight function that requires formal approval from the bank's board of directors or an appropriate board-designated committee, independent of the investment advisory function. 2178.0.

r. Real Estate Appraisals and Evaluations

» *See* Interagency Appraisal and Evaluation Guidelines described below. 2231.0.

s. General Financial and Investment Advisory Activities

» With respect to investment or financial adviser activities, examiners should determine if the board of directors has developed adequate objectives and policies. 3130.1.3.2.2.

» Inspection procedures include determining, if the board of directors does not directly supervise investment adviser activity, whether: (a) a responsible board committee(s) has been named to exercise the function; (b) there are any delegations consistent with by-law provisions and other appropriate principles; and (c) the board's minutes reflect periodic but timely review of conduct and operating results of the function;

» In addition, inspection procedures include determining whether (a) minutes of the board require and approve, where necessary, appropriate written policies, strategic plans, and management reports relating thereto; (b) the board or its committee(s) review(s) audit and regulatory reports, litigation developments, earnings and expense reports and changes to fee schedules; (c) the board, through adoption of formal policies and provisions for auditing, seeks to ensure the integrity of the organization's records and operational systems; and (d) the board or a board committee considers, periodically reviews, and provides for insurance protection. 3130.1.3.2.2.1.

» Inspection procedures for account administration include determining whether, when an investment adviser uses options and/or futures, the board of directors or a directors' level committee has approved a policy and strategy for their use. 3130.1.3.2.3.2.

t. Underwriting and Dealing in U.S. Obligations, Municipal Securities and Money Market Instruments

» Examination procedures include determining whether the board of directors, consistent with its duties and responsibilities, has:

- adopted, and reviewed at least quarterly, written securities underwriting/trading policies (and reviewed periodically that underwriting/trading department is in compliance with such policies) that outline objectives; establish limits and/or guidelines; recognize possible conflicts of interest and establish appropriate procedures; state procedures for periodic, monthly or quarterly valuation of trading inventories to market value; state procedures for periodic independent verification of valuations of the trading inventories; outline methods of internal review and reporting by department supervisors and internal auditors to ensure compliance with established policy; and identify permissible types of securities. 3240.0.13.2.

- adopted written offsetting repurchase transaction policies. 3240.0.13.2.

u. Futures Commission Merchants and Futures Brokerage

» The board, a designated subcommittee of the board, or high level of senior management should approve overall business strategies and significant policies that govern risk-taking in the organization's FCM activities. In particular, the board or a committee thereof should approve policies that identify authorized activities and managerial oversight and should articulate risk tolerances and exposure limits of FCM activities. The board should also actively monitor the performance and risk profile of its FCM activities. Directors and senior management should periodically review information that is sufficiently detailed and timely to allow them to understand and assess the various risks involved in these activities. In addition, the board or a delegated committee should periodically reevaluate the business strategies and major risk-management policies and procedures, emphasizing the organization's financial objectives and risk tolerances. 3250.0.2.1.

» Inspection procedures include determining whether the board of the FCM has approved written policies summarizing the following activities:

- the risk appropriate for the FCM, including credit, market, liquidity, operation, reputation and legal risk (*see* SR-95-51);

- the monitoring of compliance with risk parameters;

- the exchange and clearinghouse memberships; and

- the internal audit function. 3250.0.10.2.

v. Supervisory Guidance on Equity Investment and Merchant Banking Activities

» Equity investment activities require the active oversight of the board of directors and senior management of the institution that is conducting the activities. The board should approve portfolio objectives, overall investment strategies, and general investment policies that are consistent with the institution's financial condition, risk profile, and risk tolerance.

» Board-approved objectives, strategies, policies, and procedures should be documented and clearly communicated to all the personnel involved in their implementation. The board should actively monitor the performance and risk profile of equity investment business lines in light of the established objectives, strategies, and policies.

» The board of directors should also ensure that there is an effective management structure for conducting the institution's equity activities, including adequate systems for measuring, monitoring, controlling, and reporting on the risks of equity investments. The board should approve policies that specify lines of authority and responsibility for both acquisitions and sales of investments. The board should also approve limits

on aggregate investment and exposure amounts, the types of investments (for example, direct and indirect, mezzanine financing, startups, or seed financing) and appropriate diversification-related aspects of equity investments such as industry, sector, and geographic concentrations. 3909.0.2.1.

w. Insurance Sales Activities and Consumer Protection in Sales of Insurance

» Elements of a sound insurance or annuity sales program includes, among other things, directors' approval of the scope of, and written policies and procedures for, the program. 3950.0.4.1. Directors should also review complaints if they involve significant compliance issues. 3950.0.4.1.1. The board or board committee should approve agreements regarding sales efforts by third parties in such a program. 3950.0.4.1.2.

» Every component of a banking organization that engages in insurance or annuity sales activities should have board-approved policies and procedures for handling customer complaints related to these sales. The customer complaint process should provide for the recording and tracking of all complaints and require periodic reviews of complaints by compliance personnel. A BHC's or state member bank's board of directors and senior management should also review complaints if the complaints involve significant compliance issues that may pose a risk to the organization. 3950.0.4.1.1.

x. Rating the Adequacy of Risk-Management Processes and Internal Controls of Bank Holding Companies

» A bank holding company's audit committee or board of directors should review the effectiveness of internal audits and other control review activities regularly. 4070.1.1.4.

y. Country Risk

» The board of directors should periodically receive reports on the level of foreign exposures and the results of stress-tests on foreign exposures. 4090.0.2.3; 4090.0.2.8. Country exposure limits should be approved by the board of directors or a board committee. 4090.0.2.6.

z. Other Supervisory Issues

» *See* Interagency Policy Statement on Income Tax Allocation in a Holding Company Structure described below. 5010.35.3.

3. Commercial Bank Examination Manual

The Foreword to the Commercial Bank Examination Manual notes that the Manual's goal is "to organize and formalize longstanding examination objectives and procedures that provide guidance to the examiner, and to enhance the quality and consistent application of examination procedures." The Foreword further notes that "[t]he materiality and significance of a given area of bank operations are the examiner's primary considerations in deciding the scope of the examination and the procedures to be performed."

a. Consolidated Supervision Framework for Large Financial Institutions

» In order for a firm to be sustainable under a broad range of economic, operational, legal or other stresses, its board of directors (or equivalent for the U.S. operations of FBOs) should provide effective corporate governance with the support of senior management. The board is expected to establish and maintain the firm's culture, incentives, structure, and processes that promote its compliance with laws, regulations, and supervisory guidance. Each firm's board of directors and committees, with support from senior management, should:

- Maintain a clearly articulated corporate strategy and institutional risk appetite. The board should set direction and oversight for revenue and profit generation, risk management and control functions, and other areas essential to sustaining the consolidated organization.

- Ensure that the firm's senior management has the expertise and level of involvement required to manage the firm's core business lines, critical operations, banking offices, and other material entities. These areas should receive sufficient operational support to remain in a safe and sound condition under a broad range of stressed conditions.

- Maintain a corporate culture that emphasizes the importance of compliance with laws and regulations and consumer protection, as well as the avoidance of conflicts of interest and the management of reputational and legal risks.

- Ensure the organization's internal audit, corporate compliance, and risk management and internal control functions are effective and independent, with demonstrated influence over business-line decision making that is not marginalized by a focus on short-term revenue generation over longer-term sustainability.

- Assign senior managers with the responsibility for ensuring that investments across business lines and operations align with corporate strategies, and that compensation arrangements and other incentives are consistent with the corporate culture and institutional risk appetite.

- Ensure that management information systems (MIS) support the responsibilities of the board of directors to oversee the firm's core business lines, critical operations, and other core areas of supervisory focus. (1005.1)

b. Internal Control and Audit Function, Oversight and Outsourcing

» The board of directors and senior managers of an institution are responsible for ensuring that the system of internal control is effective. Their responsibility cannot be delegated to others within or outside the organization. Even when outsourcing vendors provide internal audit services, the board of directors and senior management of an institution are responsible for ensuring that both the system of internal control and the internal audit function operate effectively. In any outsourced internal audit arrangement, the institution's board of directors and senior management must maintain ownership of the internal audit function and provide active oversight of outsourced activities. (1010.1)

c. Due from Banks

» Examination procedures include determining whether the board, consistent with its duties and responsibilities, has adopted written policies for due from bank accounts and whether the board, or the board's designee, has reviewed at least annually the policies in light of changing conditions. (2010.4)

d. Interbank Liabilities

» The board of directors must review annually the internal policies and procedures that evaluate the credit and liquidity risks, including operational risks, in selecting correspondents and terminating those relationships. (2015.1)

e. Investment Securities and End User Activities

» Equity investment activities require the active oversight of the board of directors and senior management of the depository institution that is conducting the private equity investment activities. The board should approve portfolio objectives, overall investment strategies, and general investment policies that are consistent with the institution's financial condition, risk profile, and risk tolerance.

» The board also should ensure that there is an effective management structure for conducting the institution's equity activities, including adequate systems for measuring, monitoring, controlling, and reporting on the risks of equity investments. The board should approve policies that specify lines of authority and responsibility for both acquisitions and sales of investments. The board should also approve (1) limits on aggregate investment and exposure amounts; (2) the types of investments (for example, direct and indirect, mezzanine financing, start-ups, seed financing); and (3) appropriate diversification-related aspects of equity investments such as industry, sector, and geographic concentrations.

» The board of directors should approve market-risk exposure limits that specify percentage changes in the economic value of capital and, when applicable, in the projected earnings of the institution under various market scenarios. (2020.1)

f. Counterparty Credit Risk Management

» *See* Interagency Supervisory Guidance on Counterparty Credit Risk Management described below. (2025.1)

g. Bank Dealer Activities

» For risk management to be effective, the board and senior management must: be active participants in the process, ensure that adequate policies and risk-tolerance limits are developed for managing the risk in bank dealer activities, and understand, review, and approve these limits across all established product lines. (2030.1)

h. Loan Portfolio Management

» The board of directors, in discharging its duty to both depositors and shareholders, must ensure that loans in the bank's portfolio are made based on the following three objectives:

- to grant loans on a sound collectible basis;
- to invest the banks funds profitably for the benefit of shareholders and the protection of depositors; and
- to serve the legitimate credit needs of the bank's community. (2040.1)

i. Concentration of Credit

» The bank's board of directors is responsible for establishing appropriate risk parameters and for monitoring exposure, as well as for evaluating the methods used by management to manage and control concentration risk. (2050.1)

j. Allowance for Loan and Lease Losses (ALLL)

» *See* Interagency Policy Statement on the Allowance for Loan and Lease Losses described below. (2070.1)

k. Commercial and Industrial Loans

» Examination procedures include determining whether the board, consistent with its duties and responsibilities, has adopted written commercial loan policies that establish procedures for reviewing commercial loan applications; define qualified borrowers; and establish minimum standards for documentation. (2080.4)

l. Real Estate Loans

» The FRB's Regulation H requires an institution to adopt real estate lending policies that are reviewed and ap-

proved by the bank's board of directors at least annually.

» Lending policies should include requirement that management monitor the loan portfolio and provide timely and adequate reports to the bank's board of directors.

» The bank's lending policies should reflect the level of risk that is acceptable to its board of directors and should provide clear and measurable underwriting standards that enable the bank's lending staff to evaluate all relevant credit factors.

» In the course of monitoring compliance with its own real estate lending policy, bank management should report to its board of directors loans of a significant size that are exceptions to bank policy.

» A bank's nonconforming loans—those in excess of the supervisory LTV limits— should be identified in bank records, and the aggregate amount, along with the performance experience of the portfolio, should be reported at least quarterly to the bank's board of directors. (2090.1)

m. Real Estate Construction Loans

» The board of directors is responsible for reviewing and adopting policies and procedures that establish and maintain an effective, independent real estate appraisal and evaluation program for all of its lending functions. (2100.1)

n. Floor Plan Loans

» Examination procedures include determining whether the board, consistent with its duties and responsibilities, has adopted, and reviewed at least annually, written floor plan loan policies that: establish procedures for reviewing floor plan applications; define qualified borrowers, overall limits, and types of merchandise to be floor planned; establish minimum standards for documentation; and establish curtailment amounts and time limits.

» While reviewing information relating to insiders that is received from the bank or appropriate examiner (including loan participations, loans purchased and sold, and loan swaps), examination procedures include determining ,if prior approval by the bank's board was required for a loan to an insider, whether such approval was obtained. (2110.4)

o. Direct Financing Leases

» Examination procedures reviewing the minutes of the meetings of the board and executive committees to determine whether purchases of property and delinquent leases are reported to the board.

» Examination procedures include determining whether the board, consistent with its duties and responsibilities, has adopted, and reviewed at least annually, written direct lease financing policies that: establish procedures for reviewing direct lease financing applications; define qualified property; and establish minimum standards for documentation.

» Examination procedures include determining whether modifications of lease terms require the approval of the board or committee that initially approved the lease.

» Examination procedures include determining whether reports listing past-due leases and/or those receiving special attention submitted to the board for review at their regular meetings. (2120.4)

p. Consumer Credit

» Examination procedures include determining whether the board, consistent with its duties and responsibilities, has adopted written installment-loan policies that

establish: procedures for reviewing installment loan applications; standards for determining credit lines; and minimum standards for documentation. (2130.4)

q. Agricultural Loans

» The board should ensure that appropriate written guidance is provided for management in the agriculture lending areas.

» Agricultural loan policies should be reviewed by the bank's board of directors and modified when deemed necessary. (2140.1)

r. Asset-Based Lending

» Examination procedures include determining whether the board, consistent with its duties and responsibilities, has adopted written accounts receivable financing policies that: establish procedures for reviewing accounts receivable financing applications; establish standards for determining credit lines; establish standards for determining percentage advance to be made against acceptable receivables; define acceptable receivables; establish minimum requirements for verification of borrower's accounts receivable; and establish minimum standards for documentation. (2160.4)

s. Securities Broker and Dealer Loans

» Examination procedures include determining whether the board, consistent with its duties and responsibilities, has adopted written loan policies that: establish standards for determining broker and dealer credit lines; and establish minimum standards for documentation. (2170.4)

t. Factoring

» Examination procedures include determining whether the board, consistent with its duties and responsibilities, has adopted, and reviewed at least annually, written factoring policies that:

- Establish procedures for reviewing factoring agreements.
- Establish standards for determining client credit lines for each of the various types of accommodations available (i.e., factored receivables, client-risk receivables, overadvances, term loans, etc.).
- Establish standards for determining individual customer limits.
- Require a client to contact the factor for approval before filling a sales order on credit terms.
- Establish standards for approving the sales orders referred to above.
- Establish standards for determining the percentage of advance that will be made against acceptable receivables in advance factoring arrangements.
- Establish standards for determining the discount on factored receivables and the interest rate or fee charged for other credit accommodations.
- Establish minimum standards for documentation. (2180.4)

u. Deposit Accounts

» A bank's board of directors (or a committee appointed by the board) should review the basis on which service charges on dormant accounts are assessed and should document the review.

» It is the board of directors' responsibility to review overdrafts as they would any other extension of credit (3000.1)

v. Borrowed Funds

» Examination procedures include determining whether the board has adopted a written policy that:

- outlines the objectives of bank borrowings;
- describes the bank's borrowing philosophy relative to risk considerations (i.e., leverage/growth, liquidity/income);
- provides for risk diversification in terms of staggered maturities rather than solely on cost;
- limits borrowings by amount outstanding, specific type or total interest expense;
- limits or restricts execution of borrowings by bank officers;
- provides a system of reporting requirements to monitor borrowing activity;
- requires subsequent approval of transactions; and
- provides for review and revision of established policy at least annually. (3010.4)

w. Assessment of Capital Adequacy

» The bank's board of directors and senior management should be encouraged to establish capital levels and ratios that are consistent with the bank's overall financial profile. (3020.1)

x. Liquidity Risk

» *See* Interagency Policy Statement on Funding and Liquidity Risk Management described below. In addition, the Manual states that the board should ensure that it understands and approves those elements of liquidity-risk management policies that articulate the institution's general strategy for managing liquidity risk, and establishes acceptable risk tolerances. (4020.1)

y. Asset Securitization

» The board of directors and senior management are responsible for ensuring that they fully understand the degree to which the organization is exposed to the credit, market, liquidity, operational, legal, and reputational risks involved in the institution's securitization activities.

- They are also responsible for ensuring that the formality and sophistication of the techniques used to manage these risks are commensurate with the nature and volume of the organization's activities. The board should approve all significant policies relating to the management of risk arising from securitization activities and should ensure that risk exposures are fully incorporated in board reports and risk management reviews. (4030.1)

z. Information Technology

» The board of directors should oversee the institution's development, implementation, and maintenance of the information security program and also approve written information security policies and programs. (4060.1)

aa. Dividends

» Declaration of a dividend requires formal action by the

board of directors to designate the medium of payment, dividend rate, shareholder record date, and date of payment. (4070.1)

bb. Interest Rate Risk Management

» The board of directors has the ultimate responsibility for the level of interest rate risk ("IRR") taken by the institution. The board should:

- approve business strategies and significant policies that govern or influence the institution's interest-rate risk;
- articulate overall IRR objectives;
- ensure the provision of clear guidance on the level of acceptable IRR;
- approve policies and procedures that identify lines of authority and responsibility for managing IRR exposures;
- monitor the performance and IRR profile of the institution and periodically review information that is timely and sufficiently detailed to allow directors to understand and assess the IRR facing the institution's key portfolios and the institution as a whole. The frequency of these reviews depends on the sophistication of the institution, the complexity of its holdings, and the materiality of changes in its holdings between reviews;
- periodically review significant IRR management policies and procedures, as well as overall business strategies that affect the institution's IRR exposure;
- ensure that the institution has personnel available who have the necessary technical skills and that senior management fully understands the risks incurred by the institution and is sufficiently controlling them. (4090.1)

cc. Contingent Claims from Off-Balance-Sheet Credit Activities

» Maintaining adequate written policies and procedures and monitoring letters of credit activities are part of the fiduciary and oversight responsibilities of the board of directors. (4110.1)

dd. Payment System Risk and Electronic Funds Transfer Activities

» The board is responsible for reviewing and approving the institution's self-assessment and recommended net debit cap category at least once each 12-month period. (4125.2)

ee. Private Placements

» A commercial bank's board of directors assumes additional responsibilities when private placement services are offered. Private-placement activities, like any other banking function, should be subject to adequate safeguards and policy considerations.

» When drafting a policy, the board of directors should ensure that self-dealing practices or conflict-of-interest charges cannot develop.

- Procedures should be developed to monitor private-placement activity whenever such services are provided by the bank or a subsidiary. Moreover, procedures should be in effect to detect any transactions that could have an adverse effect on the bank's other functions, such as loan or trust department activities. (4130.1)

ff. Real Estate Appraisals and Evaluations

» *See* Interagency Appraisal and Evaluation Guidelines described below. (4140.1)

gg. Retail Sales of Nondeposit Investment Products

» *See* Interagency Statement on Retail Sales of Nondeposit Investment Products described below. (4170.1)

hh. Duties and Responsibilities of the Directors

» **SELECTION OF COMPETENT EXECUTIVE OFFICERS:** One of the board's most important duties is to select and appoint executive officers who are qualified to administer the bank's affairs effectively and soundly. The board is also responsible for removing officers who do not meet reasonable standards of honesty, competency, executive ability, and efficiency.

» **EFFECTIVE SUPERVISION OF BANK AFFAIRS:** The type and degree of supervision required of a bank's board of directors to ensure a bank is soundly managed involve reasonable business judgment and competence and sufficient time to become informed about the bank's affairs. Directors ultimately are responsible for the soundness of the bank.

» **ADOPTION AND ADHERENCE TO SOUND POLICIES AND OBJECTIVES:** The directors' role is to provide a clear framework of objectives and policies within which the chief executive officer can operate and administer the bank's affairs. This framework is often accomplished through the use of strategic plans and budgets. The board of directors is responsible for establishing the policies that govern and guide the day-to-day operations of the bank, so they should review and approve them from time to time.

» **AVOIDANCE OF SELF-SERVING PRACTICES:** A bank's directors bear a greater than normal responsibility for upholding safe and sound practices in dealing with transactions involving other members of the directorate and their related interests. Directors' decisions must preclude the possibility of partiality or favored treatment. Unwarranted loans to a bank's directors or their interests can be a serious safety and- soundness concern for the bank.

» **AWARENESS OF THE BANK'S FINANCIAL CONDITION AND MANAGEMENT POLICIES:** The board or a committee designated by the board should review the audit reports with the bank's management and the independent public accountants.

» **MAINTENANCE OF REASONABLE CAPITALIZATION:** A board of directors has the responsibility for maintaining its bank on a sufficiently capitalized basis.

» **COMPLIANCE WITH BANKING LAWS AND REGULATIONS:** Directors must carefully observe that banking laws are not violated.

» **GUARANTEE OF A BENEFICIAL INFLUENCE ON THE COMMUNITY'S ECONOMY:** Directors have a continuing responsibility to provide those banking services which meet the legitimate credit and other needs of the community being served. Directors should be certain that the bank attempts to satisfy all legitimate credit needs of the community.

» **BOARD MEETINGS:** The board should conduct its business in meetings held as required by the bank's bylaws or state law.

» **MINUTES OF BOARD MEETINGS:** The board should ensure that an accurate, adequate record of its actions is maintained. Such a record is usually kept in the form of minutes of the board meetings. The minutes should document the board's review of all regular items mentioned above as well as the review and discussion of all significant items that are not part of the regular meeting. Additionally, at a minimum, the minutes should record the attendance or absence of each director at each meeting, detail the establishment and composition of any committees, and note the abstention of any director from any vote.

» **BOARD COMMITTEES:** Many boards elect to delegate some of their workload to committees. The extent and nature of the bank's activities and the relative expertise of each board member play key roles in the board's determination of which committees to establish, who sits on them, and how much authority they have. Thus, there is no ideal committee structure.

» **COMPLIANCE WITH FORMAL AND INFORMAL SUPERVISORY ACTIONS:** Bank directors must correct any deficiencies found in the bank. (5000.1)

4. Federal Reserve Policy on Payment System Risk (as amended effective 12/31/14)

» Each institution incurring daylight overdrafts in its Federal Reserve account must adopt a net debit cap, that is, a ceiling on the total daylight overdraft position that it can incur during any given day. At least once in each 12-month period, each institution's board of directors must review that institution's self-assessment (of its own creditworthiness, intraday funds management and control, customer credit policies and controls, and operating controls and contingency procedures) and recommended cap category.

- A cap determination may be reviewed and approved by the board of directors of a holding company parent of an institution, provided that (1) the self-assessment is performed by each entity incurring daylight overdrafts, (2) the entity's cap is based on the measure of the entity's own capital, and (3) each entity maintains for its primary supervisor's review its own file with supporting documents for its self-assessment and a record of the parent's board of directors review.

- An institution may incur daylight overdrafts of up to 40 percent of its capital measure without performing a self-assessment if the institution submits a board of directors resolution (or a resolution by its holding company's board) to its Reserve Bank at least once in each 12-month period approving the institution's use of intraday credit up to this de minimis level.

- An institution approved for a maximum daylight overdraft capacity level must submit at least once in each twelve-month period a board of directors resolution indicating its board's approval of that level.

C. FDIC

1. Pocket Guide for Directors

» A financial institution's board of directors oversees the conduct of the institution's business. The board of directors should:

- select and retain competent management;

- establish, with management, the institution's long- and short-term business objectives, and adopt operating policies to achieve these objectives in a legal and sound manner;

- monitor operations to ensure that they are controlled adequately and are in compliance with laws and policies;

- oversee the institution's business performance; and

- ensure that the institution helps to meet its community's credit needs.

» The Pocket Guide also discusses the importance of maintaining the board's independence, and of directors keeping informed of the activities and condition of the institution and of the environment in which it operates.

» The board should ensure that all significant activities are covered by clearly communicated written policies that cover, at a minimum: loans, including internal loan

review procedures; investments; asset-liability/funds management; profit planning and budget; capital planning; internal controls; compliance activities; the audit program; conflicts of interest; and the code of ethics.

- The board's policies should establish mechanisms for providing the board the information needed to monitor the institution's operations.

» The board also should establish a mechanism for independent third party review and testing of compliance with board policies and procedures, applicable laws and regulations, and accuracy of information provided by management.

- The board or its audit committee should have direct responsibility for hiring, firing, and evaluating the institution's auditors, and should have access to the institution's regular corporate counsel and staff as required.

» Board members should personally review any reports of examination or other supervisory activity, and any other correspondence from the institution's supervisors. Directors should discuss issues of concern with the examiners.

2. Statement Concerning the Responsibilities of Bank Directors and Officers

» Directors are responsible for selecting, monitoring, and evaluating competent management; establishing business strategies and policies; monitoring and assessing the progress of business operations; establishing and monitoring adherence to policies and procedures required by statute, regulation, and principles of safety and soundness; and for making business decisions on the basis of fully informed and meaningful deliberation.

» Directors must require and management must provide the directors with timely and ample information to discharge board responsibilities. Directors also are responsible for requiring management to respond promptly to supervisory criticism. Open and honest communication between the board and management of the bank and the regulators is extremely important.

3. Financial Institution Letters

a. FIL-47-2013: Director and Officer Liability Insurance Policies, Exclusions, and Indemnification for Civil Money Penalties

» The board of directors' choice of coverage in a D&O policy should be based on a well-informed analysis of costs and benefits, and an important consideration is the potential impact to directors and officers that could result from exclusions. Directors must be aware that D&O insurance policies are not allowed to cover any institution-affiliated party for the cost of civil money penalties assessed against them by a banking agency.

b. FIL-46-2013: Managing Sensitivity to Market Risk in a Challenging Interest Rate Environment

» Board oversight of interest rate risk management is essential. The board of directors has to be aware of potential interest rate risk exposure and need to have strong policies in place in order to defray the risk. The board should review its asset-liability management and investment policies annually, to ensure they reflect current realities and the risk appetite of the board.

c. FIL-20-2012: FDIC Statement on CFPB Bulletin 2012-02: Payments to Loan Originators Based on Mortgage Transaction Terms or Conditions under Regulation Z

» FDIC-supervised institutions must comply with CFPB guidance on loan originator compensation and should implement periodic reviews of the compensation pro-

gram into general compliance. Any material exceptions must be reported to the board of directors.

d. FIL-3-2012: Payment Processor Relationships Revised Guidance (Revised July 2014)

» With respect to payment processor relationships, board-approved policies and programs should assess the financial institution's risk tolerance for this type of activity, verify the legitimacy of the payment processor's business operations, determine the character of the payment processor's ownership, and ensure ongoing monitoring of payment processor relationships for suspicious activity, among other things. Policies and procedures should outline the bank's thresholds for unauthorized returns, the possible actions that can be taken against payment processors that exceed these standards, and methods for periodically reporting such activities to the bank's board of directors and senior management.

e. FIL-81-2010: Overdraft Payment Programs and Consumer Protection

» With respect to automated overdraft payment programs, the board of directors and management should ensure that the institution mitigates the associated risks and complies with all consumer protection laws and regulations, including providing clear and meaningful disclosures and other communications about overdraft payment programs, fees and other features and options, and demonstrating compliance with new opt-in requirements for automated teller machine withdrawals and one-time point-of-sale debit card transactions.

f. FIL-4-2009: Risk Management of Remote Deposit Capture

» *See* FFIEC – Risk Management of Remote Deposit Capture below.

g. FIL-44-2008: Guidance for Managing Third-Party Risk

» An institution's board of directors and senior management are ultimately responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships, to the same extent as if the activity were handled within the institution.

h. FIL-22-2008: Managing Commercial Real Estate Concentrations in a Challenging Environment

» The board of directors and management should take steps to increase capital levels to support significant commercial real estate concentrations and should strive for strong capital and loan loss allowance levels and implement robust credit risk management practices.

i. FIL-52-2006: Foreign-Based Third-Party Service Providers — Guidance on Managing Risks in These Outsourcing Relationships

» The board of directors and senior management have a responsibility to ensure that third-party service provider activity is conducted in a safe and sound manner in compliance with policies and applicable laws.

- Their responsibilities include ensuring that systems and controls are established and maintained for the security and integrity of outsourced data, whether the third-party service provider is foreign or domestic.

» The board of directors and senior management are responsible for recognizing the risks associated with the institution's outsourcing relationships with foreign-based third party service providers and adopting and implementing an effective risk management strategy.

- Of primary importance at the outset is assessing whether a relationship with a foreign-based third party service provider is consistent with the financial institution's overall business strategy.

j. FIL-64-2005: Guidance on How Financial Institutions Can Protect Against Pharming Attacks

» The effectiveness of an insured institution's Internet domain name protection program should be addressed in periodic risk assessments and status reports presented to the institution's board of directors.

k. FIL-17-2003: Corporate Governance, Audits, and Reporting Requirements

» Applicability of Selected Provisions of the Sarbanes-Oxley Act of 2002 to FDIC-Supervised Banks With Less Than $500 Million In Total Assets That Are Not Public Companies:

- If a bank is considering engaging its external auditor to perform both internal and external audit services, the bank's audit committee (or board of directors if there is no audit committee) and the external auditor should pay particular attention to preserving the independence of both the internal and external audit functions.
- In addition, if a bank is considering having its external auditor perform any of the other non-audit services prohibited by Section 201 of the Act, the FDIC encourages the bank's audit committee (or board of directors) to discuss the implications of the performance of these services on the auditor's independence.
- As a general corporate governance matter, the FDIC encourages the audit committee (or board of directors) of each bank to preapprove all audit and non-audit services to be provided by its external auditor.

l. FIL-110-98: Acquisition, Development, and Construction Lending

» The institution's board of directors is responsible for establishing appropriate risk limits, monitoring exposure, and evaluating the effectiveness of the institution's efforts to manage and control risk. When crafting internal guidelines for acquisition, development and construction and other real estate lending programs, the board should carefully consider the Interagency Guidelines for Real Estate Lending Policies, which can be found under Appendix A to Subpart A of 12 C.F.R. Part 365. In particular, the following items within the Interagency Guidelines should be noted:

- Feasibility studies and sensitivity analyses;
- Minimum initial investment and hard equity maintenance requirements;
- Minimum standards for net worth, cash flow, and debt service coverage of the borrower or the underlying property;
- Standards for the acceptability of, or limits on, non-amortizing loans and interest reserves;
- Pre-leasing and pre-sale requirements;
- Limits on partial recourse or non-recourse loans and requirements for guarantor support;
- Requirements for take-out commitments; and
- Minimum covenants for loan agreements.

» The board of directors is responsible for establishing standards for reviewing and approving exceptions to loan policy.

m. FIL-80-98: Nondeposit Investment Products

» The board should review and update its Nondeposit Investment Products (NDIP) statement whenever a material change to the NDIP program occurs. If no material change to the NDIP program occurs, the board should review its NDIP program at least annually.

n. FIL-52-95: Vacation Policies

» When the vacation policy does not conform to the recommended two-week absence, the institution's board of directors should review and approve the policy actually followed and the exceptions allowed.

4. Examination Manuals (applicable only to insured state non-member banks)

a. Risk Management Manual of Examination Policies

Section 1.1 of this Manual states that "[t]he primary purpose of this Manual is to provide policy guidance and direction to the field examiner that should be applied in the risk management examination process," also noting that "[t]he exercise of examiner judgment to determine the scope and depth of review in each functional area is crucial to the success of the risk-focused supervisory process."

(1) SECTION 3.2 – LOANS

» The board of directors of every bank has the legal responsibility to formulate lending policies and to supervise their implementation. Therefore examiners should encourage establishment and maintenance of written, up to date lending policies which have been approved by the board of directors.

- A lending policy should not be a static document, but must be reviewed periodically and revised in light of changing circumstances surrounding the borrowing needs of the bank's customers as well as changes that may occur within the bank itself.
- Among other things, lending policies should address the responsibility of the board of directors in reviewing, ratifying, or approving loans.

» Management should maintain a written loan review policy that is reviewed and approved at least annually by the board of directors.

» It is the responsibility of the board of directors and management to maintain the allowance for loan and lease losses (ALLL) at an adequate level. The allowance adequacy should be evaluated, and appropriate provisions made, at least quarterly. In carrying out their responsibilities, the board and management are expected to:

- establish and maintain a loan review system that identifies, monitors, and addresses asset quality problems in a timely manner;
- ensure the prompt charge-off of loans, or portions of loans, deemed uncollectible; and
- ensure that the process for determining an adequate allowance level is based on comprehensive, adequately documented, and consistently applied analysis.

» At least quarterly, management and the board of directors should receive comprehensive reports about the characteristics and trends in exposures to higher risk credits, including leveraged finance transactions, which require frequent monitoring by banking organizations.

» Examiners should determine whether an institution's board of directors and management have established policies for leveraged finance that minimize the risks posed by potential legal issues and conflicts of interest.

» The board of directors should review and approve an environmental risk program and designate a senior offi-

cer knowledgeable in environmental matters responsible for program implementation.

» The board and senior management should properly oversee subordinates to determine that sound lending policies are being carried out.

» Although a general resolution is perhaps satisfactory for the short term, unsecured borrowings of a corporation, a specific resolution of the corporation's board of directors is generally advisable to authorize such transactions as term loans, loans secured by security interests in the corporation's personal property, or mortgages on real estate.

- Whenever there is a question concerning a corporation's authority to guarantee a loan, counsel should be consulted and a special corporate resolution passed by the organization's board of directors.

» The board should approve arrangements with third parties to provide services that the bank would normally provide, which should be guided by written contract.

» *See also* Interagency Guidance on Subprime Lending; Interagency Appraisal and Evaluation Guidelines described below.

(2) SECTION 3.3 – SECURITIES AND DERIVATIVES

» Board oversight is vital to effective investment risk management, and the board has very specific investment activity responsibilities.[3] The board should adopt policies that establish guidelines for management and periodically review management's performance. The board should:

- Approve broad goals and risk limits,
- Adopt major investment and risk management policies,
- Understand the approved investment activities,
- Ensure competent investment management,
- Periodically review management's investment activity,
- Require management to demonstrate compliance with the board's goals and risk limits, and
- Mandate an independent review program and review its findings.
- In addition, management should develop investment strategies to achieve the board's goals and should provide periodic reports to the board.
- The board and management should periodically evaluate and, when warranted, modify the program.

» The board is responsible for adopting comprehensive written investment policies that clearly express the board's investment goals and risk tolerance.

- The policies should articulate the investment portfolio's purpose, risk limits, and return goals. Return goals should express the board's earnings objectives for the investment portfolio. The board may also establish portfolio performance targets.

» To effectively oversee investment activities, the board must approve the bank's risk limits. Management should set these risk limits, consistent with the board's goals, objectives, and risk appetite. The risk limits should be formally approved and incorporated within the board's policies.

» Market risk limits should at least quantify maximum permissible portfolio or individual instrument price sensitivity as percentage of capital or earnings. Capital-based risk limits clearly illustrate the potential threat to the bank's viability, while earnings-based limits reflect potential profitability effects. In addition, the board

3 Throughout this guidance, the terms "board" references either the board of directors or a designated board committee.

may choose to establish limits relative to earnings, total assets, total investment securities, or other standards.

» Credit risk limits should generally restrict management to investment grade instruments. The board may permit management to acquire nonrated instruments; however, these instruments should be consistent with investment grade standards. Regardless, the board should carefully monitor such activity.

» The board has responsibility for establishing general internal control guidelines, which management should translate into clear procedures that govern daily operations.

» The board should adopt policies that address authorized employees' personal relationships, including securities transactions, with the bank's approved securities broker/dealers. The board may also adopt policies that address the circumstances under which directors, officers, and employees may accept gifts, gratuities, or travel expenses from securities broker/dealers and associated personnel.

» Independent review findings should be reported directly to the board at least annually. The board should carefully review the independent review reports and ensure that material exceptions are corrected.

» Management should regularly ensure compliance with internal policies and regulatory requirements and should periodically evaluate portfolio performance. The board should review and consider each policy exception. Management should present exceptions for approval before engaging in an unauthorized activity. Recurring exceptions should prompt close scrutiny from the board. When warranted, the board may consider changing its policies to permit an activity. The board should take strong action when management fails to seek prior approval for an unauthorized activity.

» Periodically, the board and management should evaluate the risk management program to ensure that its investment activities reasonably meet the board's goals and the bank's strategic needs. Without such an assessment, the board and management cannot prudently oversee investment activities. The scope and detail of the evaluation should correspond to the bank's size, complexity, and investment activities. At most banks, annual evaluations should be sufficient. In larger or more complex banks, quarterly (or more frequent) evaluation may be necessary.

  - The board should review management's reports, including an investment activity summary, portfolio risk and performance measures, and independent review findings to identify broad weaknesses.

  - The board should first consider the bank's current and expected condition, competitive environment, and strategic plans. Then, the board should reassess its portfolio goals to ensure that they do not conflict with the overall strategic plan. When necessary, the board should adjust its portfolio goals.

» Investment authority may be delegated to a third party with specific board approval.

(3) SECTION 3.4 – CASH AND DUE FROM BANKS

» Proper controls for structured CD investments include effective senior management supervision, board oversight, periodic reporting, and appropriate policies and procedures.

(4) SECTION 3.7 – OTHER ASSETS AND LIABILITIES

» The safe and sound use of bank-owned life insurance ("BOLI") depends on effective senior management and board oversight. An institution's board of directors must understand the complex risk characteristics of the institution's insurance holdings and the role this asset plays in the institution's overall business strategy.

» The board of directors or appropriate committee thereof should approve an acquisition of bank-owned life insurance in an amount that results in an aggregate cash surrender value in excess of 25 percent of the institution's Tier 1 capital, or any lower internal limit.

» Management should analyze the financial condition of BOLI insurance carriers, review the performance of BOLI products, and report their findings to the board at least annually.

(5) SECTION 3.8 – OFF-BALANCE SHEET ACTIVITIES

» Banks with a material level of contingent liabilities should have written policies addressing such activities adopted and approved by their board of directors.

(6) SECTION 4.1 – MANAGEMENT

» It is a primary duty of a board of directors to select and appoint executive officers who are qualified to administer the bank's affairs effectively and soundly. It is also the responsibility of the board to dispense with the services of officers who prove unable to meet reasonable standards of executive ability and efficiency.

» The board of directors is charged with the responsibility of conducting the affairs of the bank. It is not expected to directly carry out details of the bank's business; these may be delegated to senior officers.

» Board members cannot be expected to be personally knowledgeable of all laws and regulations, but they should make certain that compliance with all laws and regulations receives high priority and violations are not knowingly committed by themselves or anyone the bank employs.

» The board of directors has the responsibility of maintaining an adequately capitalized bank, and once this responsibility has been satisfied, the payment of dividends can and should receive consideration.

» A sound framework of internal controls and a reliable and objective audit function are essential tools for bank directors. The existence of such enable directors to remain well informed of the adequacy, effectiveness, and efficiency of accounting, operating, and administrative controls and provide an assessment of the quality of ongoing operations. Establishment and oversight of such controls is the responsibility of the board of directors.

» Supervision by directors does not necessarily indicate a board should be performing management tasks, but rather ensuring that its policies are being implemented and adhered to and its objectives achieved. It is the failure to discharge these supervisory duties which has led to bank failures and personal liability of directors for losses incurred.

- Directors' supervisory responsibilities can best be discharged by establishing procedures calculated to bring to their attention relevant and accurate information about the bank in a consistent format and at regular intervals.
    - *From this critical point, the remainder of a director's job unfolds. Directors who keep abreast of basic facts and statistics such as resource growth, capital growth, loan-to-deposit ratios, deposit mix, liquidity position, general portfolio composition, loan limits, loan losses and recoveries, delinquencies, etc., have taken a first, indispensable step in discharging their responsibilities.*
    - *It is essential, therefore, that directors insist on receiving pertinent information about the bank in concise, meaningful and written form, and it is one of executive management's most important responsibilities to make certain directors are kept fully informed on all important matters and that the record clearly reflects this.*
- Directors' meetings that are conducted in a businesslike and orderly manner are a significant aid to fulfillment of the board's supervisory responsibilities. This requires, among other things, regular attendance (whether by actual or audio, video or other remote access).

- *Absence without just cause is, like ignorance, not a valid defense. Moreover, a director's attendance should be an informed and intelligent one, and the record should reflect this.*

- *If directors dissent from the majority, they should, for their own protection, insist upon their negative vote being recorded along with reasons for their action.*

- To carry out its functions, the board of directors may appoint and authorize committees to perform specific tasks and supervise certain phases of operations.

  - *In most instances, the name of the committee, such as loan, investment, examination, and, if applicable, trust, identifies its duties.*

  - *Of course, utilization of the committee process does not relieve the board of its fundamental responsibilities for actions taken by those groups. Review of the minutes of these committees' meetings should be a standard part of the board meeting agenda.*

- Communication of facts to a board of directors is essential to sound and effective supervision. However, with the ever-broadening scope of modern banking and the increased complexity of banking operations, the ability of a board of directors to effectively supervise is becoming more difficult.

  - *Because of this, the use of outside personnel to provide management supervision is relatively common. While this does not release the board from its legal and implied responsibilities, it does provide an opportunity for management improvement through the use of these external sources.*

» In general, directors and other corporate officers of a bank may be held personally liable for: a breach of trust; negligence which is the proximate cause of loss to the bank; ultra vires acts, or acts in excess of their powers; fraud; and misappropriation or conversion of the bank's assets.

- A director's duty to exercise due care and diligence extends to the management, administration and supervision of the affairs of the bank and to the use and preservation of its assets. Perhaps the most common dereliction of duty by bank directors is the failure to maintain reasonable supervision over the activities and affairs of the bank, its officers and employees.

» The board should be encouraged to act specifically on any loan or other transaction in which insiders or their associates may be involved, either directly or indirectly, or because of business associations outside the loan or transaction in question.

» In all cases, the bank's directors and shareholders should be fully informed regarding the nonbanking activity conducted on bank premises. The operation should be approved by the bank's shareholders, and expenses incurred by the bank in connection with these operations formally approved by the board of directors annually.

» Examiners should review the information used by the board to establish the compensation structure of the institution. The information should adequately explain the rationale for the system in place and should enable the board to consider the above items that determine whether compensation is excessive.

(7) SECTION 4.2 – INTERNAL ROUTINE AND CONTROLS

» The board of directors is responsible for ensuring internal control programs operate effectively. Their oversight responsibilities cannot be delegated to others within the institution or to outside parties. The board may delegate operational activities to others; however, the board must ensure effective internal control programs are established and periodically modified in response to changes in laws, regulations, asset size, organizational complexity, etc.

» A bank's board and senior management are responsible for developing effective internal control systems

and ensuring all personnel understand and respect the importance of internal controls.

» The board of directors or an audit committee preferably consisting entirely of outside directors (directors independent of operational duties), must monitor adherence to established directives regarding control standards. Boards should establish policy standards that address issue such as decision-making authorities, segregation of duties, employee qualifications, and operating and recording functions.

» The board of directors should establish limits for all significant matters (such as lending and investment authorities) delegated to relevant committees and officers. Management should regularly provide financial and operational reports to the board, including standardized reports that detail policy exceptions, new loans, past due credits, concentrations, overdrafts, security transactions, etc. The board or a designated board committee should periodically review all authority levels and material actions. The key control objective is that the board is regularly informed of all significant matters.

(8) SECTION 4.3 – RELATED ORGANIZATIONS

» The board of directors is responsible for actively overseeing the affairs of the institutions. This oversight should include:

- Reviewing and approving major corporate actions and the institution's overall corporate strategies, business plans, performance objectives, risk policies and risk tolerances,
- Monitoring the institution's adherence to the strategies, plans, objectives, risk policies and risk tolerances approved by the board, including policies and standards relating to conflicts of interest management,
- Reviewing appropriate regulatory and audit reports, and
- Taking appropriate action with respect to all matters requiring board attention.

» The board of directors is responsible for ensuring that the institution, its directors, management, principal shareholders, and affiliates avoid potential direct and indirect conflicts of interest and comply with Federal laws and regulations that are designed to prevent misuse of depositors' funds.

» The board of directors is responsible for hiring and retaining executive officers with the skills, integrity, knowledge and expertise appropriate to the nature and scope of their responsibilities.

» The board of directors is responsible for establishing and maintaining appropriate committees, and that written charters delineating each committee's functions, responsibilities and membership qualifications have been adopted by the full board.

» The board of directors is responsible for ensuring that the insured depository institution maintains a separate corporate existence from its affiliates. This separateness also pertains to the sound tenet that all financial and other pertinent records for the financial institution affiliate be accessible on location.

» A formal written employee sharing agreement should be established to define the employment relationship between the banking entity and affiliate; the board should review the agreement to ensure that it is fair and in the best interest of the insured bank.

(9) SECTION 4.4 – FIDELITY AND OTHER INDEMNITY PROTECTION

» The board of directors must determine the maximum loss the bank is willing and able to assume, and should perform an annual review of the bank's risk and insurance management program.

» While a periodic review of internal and external security measures and controls is warranted in every bank, it is especially appropriate in a bank that is operating without fidelity insurance coverage. Ideally, this effort should be undertaken as a special project with responsibility fixed in a particular executive officer. Further, it should include a comprehensive review of the bank's existing programs, the design and implementation of additional security procedures and controls, and a formal report to the board of directors, with any actions taken by the board based on the report findings noted in the minutes of the meeting.

(10) SECTION 5.1 – EARNINGS

» Holding companies and subsidiary institutions are encouraged to enter into a written, comprehensive tax allocation agreement tailored to their specific circumstances. The agreement should be approved by the respective boards of directors.

(11) SECTION 6.1 – LIQUIDITY AND FUNDS MANAGEMENT

» Board oversight is critical to effective liquidity risk management. The board is responsible for establishing the institution's liquidity risk tolerance and clearly communicating it to all levels of management. Additionally, the board should review, approve, and periodically update liquidity management strategies, policies, procedures, and risk limits. To be effective, the board should ensure it:

- Understands and periodically reviews the institution's current liquidity position and contingency funding plans;
- Understands the institution's liquidity risks and periodically reviews information necessary to maintain this understanding;
- Establishes an asset/liability committee (ALCO) and guidelines for electing committee members, assigning responsibilities, and establishing meeting frequencies;
- Establishes executive-level lines of authority and responsibility for managing the institution's liquidity risk;
- Provides appropriate resources to management for identifying, measuring, monitoring, and controlling liquidity risks; and
- Understands the liquidity risk profiles of significant subsidiaries and affiliates.

» Management is also responsible for regularly reporting the institution's liquidity risk profile to the board.

» At least annually, boards should review and approve appropriate liquidity policies.

» Management and the board should establish meaningful risk limits and periodically evaluate the appropriateness of established limits.

» Given the critical role assumptions play in measuring liquidity risks and cash flow projections, management should ensure all key assumptions are appropriate and well documented, and the board should periodically review and formally approve the assumptions used. The board and management should also closely review the assumptions used to assess the liquidity risk of complex assets, liabilities, and off-balance sheet positions.

(12) SECTION 7.1 – SENSITIVITY TO MARKET RISK

» Effective board oversight is the cornerstone of sound risk management. The board of directors is responsible for overseeing the establishment, approval, implementation, and annual review of interest rate risk ("IRR") management strategies, policies, procedures, and risk limits. The board should understand and regularly review reports that detail the level and trend of the institution's IRR exposure.

» The board or an appropriate board committee should review sensitivity to market risk information at least

quarterly. The information should be timely and of sufficient detail to allow the board to assess senior management's performance in monitoring and controlling market risks and to assess management's compliance with board-approved policies.

» In order to fulfill its responsibilities in this area, the board is expected to:

- Establish formal risk management policies, strategies, and risk tolerance levels;
- Define management authorities and responsibilities;
- Communicate its risk management strategies and risk tolerance levels to all responsible parties;
- Monitor management's compliance with board-approved policies;
- Understand the bank's risk exposures and how those risks affect enterprise-wide operations and strategic plans; and
- Provide management with sufficient resources to measure, monitor, and control IRR.

» Examiners should carefully evaluate policy guidelines and board-approved risk limits.

(13) SECTION 8.1 – BANK SECRECY ACT, ANTI-MONEY LAUNDERING, AND OFFICE OF FOREIGN ASSETS CONTROL

» Institutions must have board-approved anti-money laundering and Bank Secrecy Act (BSA) compliance programs. Best practices dictate that board should review and approve the BSA compliance policy annually.

(14) SECTION 11.1 – INTERNATIONAL BANKING

» The board should approve policy guidelines regarding exit strategies (action plans) with defined trigger points to effect the reduction of exposure in a given country portfolio when conditions warrant.

- Once exit strategies are employed, monthly or quarterly reporting should be provided to the bank's board of directors to update the board on the ongoing nature of exposure and progress towards reducing and/or limiting risk.

» Every bank engaged in international lending should be guided by a formal statement of policy approved by its board of directors. Content will vary depending on the size of the bank and the extent of its international commitment, but certain factors should be addressed in almost all situations.

- These would most often include a summary of management's basic credit standards, a statement of the bank's international lending objectives, a description of its system for credit approval, a recital of loan processing procedures, and establishment of specific personnel lending authorities.
- In addition, the policy should establish procedures that ensure that the board of directors will regularly be apprised of the condition of the international loan portfolio. It will be appropriate to indicate the major differences in international versus domestic lending.

b. Credit Card Activities Manual

The Introduction to this Manual states that it "is intended to assist examiners in gaining a broad understanding of the unique characteristics of bank credit card operations," also noting that "examination approaches necessary to assess credit card operations may require augmentation or modification beyond the approaches provided in this manual, depending on circumstances that arise."

(1) CHAPTER IV, CREDIT CARD PROGRAM DEVELOPMENT

» The board of directors is responsible for conducting the

bank's affairs, including credit card activities.

» A vital part of the board's responsibilities is to set the future direction of the bank, and sound planning is indispensable in dealing with the uncertainty and rapid change that permeates the credit card industry.

» Examiners should identify whether the board has ensured that management and staff possess sufficient expertise to appropriately manage the risks involved with credit card lending and that staffing levels are adequate for the planned volume and complexity of the activity.

» When determining an appropriate organizational structure in relation to planned activities, the board often appoints and authorizes committees to perform specific tasks and supervise certain phases of credit card operations.

» Examiners should evaluate whether the committee structure reflects careful consideration by the board for ensuring that it is effective and adds value to the organization. Use of committees does not relieve the board of its fundamental responsibilities for actions taken by those groups.

  • Review of committee meeting minutes commonly is not only a standard part of board meetings, but of examinations as well. Examiners review the committee structure (including charters and member lists) and sample the committee minutes to determine whether the board has provided a valuable committee structure that is consistent with the size, complexity, and nature of the bank and its credit card activities and that each committee is effectively fulfilling its role.

» Examiners should verify the board's practices for ensuring that it receives pertinent information about the bank's credit card operations in concise, meaningful, and written form and management's practices for making certain that directors are kept fully informed on all important matters and that the records clearly reflect this.

» Examiners expect directors to remain well informed of the adequacy, effectiveness, and efficiency of accounting, operating, and administrative controls as well as the quality of ongoing credit card operations. Examiners should determine whether the board has carefully considered the extent of auditing needed to effectively monitor operations, internal controls, and financial reporting. Proper determination of necessary audit resources, either internal or external, considers the nature, complexity, and risk profile of the credit card activities as well as of the bank itself.

(2) CHAPTER XIV, CREDIT CARD ISSUING RENT-A-BINS (RENT-A-BANK IDENTIFICATION NUMBER)

» Examiners should see proof that the board of directors has assigned responsibility both for evaluating the financial information provided by Rent-a-BIN partners and for reporting the findings to the board (or a designated committee) to competent employees.

(3) CHAPTER XV, LIQUIDITY

» Examiners should confirm whether the bank has board-approved written policies and procedures for day-to-day liquidity management as well as MIS adequate to measure, monitor, control and report liquidity risk.

c. Credit Card Securitization Manual

The Introduction to this Manual states that it "is intended to assist examiners in understanding and evaluating the credit card securitization process."

(1) CHAPTER VIII, RESIDUAL INTERESTS VALUATION AND MODELING

» Examiners should expect the board to have approved an effective validation policy and review the policy for adequacy. The validation policy should set forth the required validation processes and procedures, scope,

frequency, reporting, documentation requirements, and responsibilities. It should also include tolerance limits for differences between projections and actual outcomes plus any remedial actions required if the discrepancies fall outside of the policy limits.

- Validation of the valuation process should focus on each element of the valuation, such as cash flow assumptions, discount rate, and model construction. Management should be completing a full, comprehensive validation process at least annually, which should be fully documented and reported to the board of directors or the audit committee.

(2) CHAPTER X, RISK MANAGEMENT AND EXAMINATION ISSUES

» Examiners should expect management and the board to:

- Have the requisite knowledge of the effects of securitization on the risk profile of the bank and be fully aware of the accounting, legal, and risk-based capital nuances associated with this activity.
- Understand the impact market and economic conditions will have on the nature of the risks inherent to securitization activities.
- Identify and clearly understand those risks that remain with the bank after the credit card receivables have been transferred to investors and credit enhancement providers.
- Fully and accurately distinguish and measure the risks that have been transferred versus those that have been retained and adequately manage both the retained and sold portions.

d. FDIC Compliance Examination Manual

The Introduction to this Manual states that it is "designed as a reference tool for Compliance examination staff to use when conducting Compliance and Community Reinvestment Act (CRA) examinations and other supervisory activities. The detailed procedures presented in the Manual are not intended to replace sound judgment and discretion on the part of examination staff."

(1) SECTION II.1.1, OVERVIEW OF COMPLIANCE EXAMINATIONS

» The FDIC examination approach appropriately recognizes that the board of directors and management of a financial institution are responsible for complying with all federal consumer protection laws and regulations. While the formality and complexity of compliance management systems will vary greatly among institutions, the FDIC expects the board of directors and management of each institution to have a system in place to effectively manage its compliance risk, consistent with its size and product mix.

» Examination procedures include evaluating:

- the commitment of the board, management and staff to compliance; and
- the responsiveness of the board and management to the findings of internal/external reviews and to the findings of the previous examination.

(2) SECTION. II.3.1, COMPLIANCE MANAGEMENT SYSTEM

» The board of directors of a financial institution is ultimately responsible for developing and administering a compliance management system that ensures compliance with federal consumer protection laws and regulations. To a large degree, the success of an institution's compliance management system is founded on the actions taken by its Board and senior management. Key actions that a board and management may take to demonstrate their commitment to maintaining an effective compliance management system and to set a

positive climate for compliance include:

- demonstrating clear and unequivocal expectations about compliance, not only within the institution, but also to third-party providers;
- adopting clear policy statements;
- appointing a compliance officer with authority and accountability;
- allocating resources to compliance functions commensurate with the level and complexity of the institution's operations;
- conducting periodic compliance audits; and
- providing for recurrent reports by the compliance officer to the board.

» The board and senior management should discuss compliance topics during their meetings and should include compliance matters in their communications to institution personnel and the general public.

» Regardless of size or institution complexity, the first step a board of directors and senior management should take in providing for the administration of the compliance program is the designation of a compliance officer.

- In developing the organizational structure of the compliance program, the board and senior management must grant a compliance officer sufficient authority and independence to cross department lines, have access to all areas of the institution's operations and effect corrective action.
- A compliance committee, as an alternative to or in addition to a full-time compliance officer, could be formed consisting of the compliance officer, representatives from various departments, and member(s) of senior management or the board. However, the ultimate responsibility of overall compliance with all statutes and regulations resides with the board.

» If an institution engages the services of a third party, the board and management must ensure that the third-party operations, products, services and activities are reviewed for compliance with consumer protection laws and regulations.

» The board should determine the scope of a consumer protection law and regulation compliance audit, and the frequency with which audits are conducted.

» Regardless of whether audits are conducted by institution personnel or by a contractor, the audit findings should be reported directly to the board of directors or a committee of the Board. Board and senior management response to the audit report should be prompt.

(3) SECTION V.9.1, COMPLIANCE LENDING ISSUES, HOME MORTGAGE DISCLOSURE ACT (HMDA)

» Examiners are to evaluate whether the institution's informal procedures and internal controls are adequate to ensure compliance with HMDA and Regulation C, including whether the board has established independent review of the policies, procedures, and HMDA data to ensure compliance and accuracy, and is advised each year of the accuracy and timeliness financial institution's data submissions.

(4) SECTION II.5.1, COMPLIANCE EXAMINATIONS

» The Examiner-in-Charge off-site review should be used to preliminarily determine whether the institution's board and management identify, understand and adequately control the elements of risks facing the financial institution.

(5) SECTION III.1.1, COMPLIANCE PRE-EXAMINATION INFORMATION PACKET

» Examiners will evaluate the bank's Compliance Man-

agement System ("CMS"), which is comprised of three main elements: board and management oversight, the compliance program, and compliance audit.

- Board and management oversight is evaluated by determining the level of attention and oversight the Board and senior management give to compliance-related responsibilities and the administration of the CMS.

(6) SECTION VIII.2.1, PRIVACY AND CONSUMER INFORMATION, CHILDREN'S ONLINE PRIVACY PROTECTION ACT (COPPA)

» Examination procedures include assessing the quality of the institution's compliance risk management by determining whether procedures and controls ensure compliance with COPPA. As part of this assessment, examiners are to consider the board of director's adoption, and management and implementation, of policies and procedures.

(7) SECTION IX-1.1, RETAIL INVESTMENT SALES

» *See* Interagency Statement on Retail Sales of Nondeposit Investment Products described below.

(8) SECTION IX-2.1, RETAIL INSURANCE SALES

» In evaluating the bank's compliance management system as it pertains to retail insurance sales activities to determine whether risks are adequately managed, examiners should consider:

- whether the bank's board of directors have adopted written policies and procedures for the bank's insurance sales program, and if not, whether they are needed;
- whether such policies and procedures are reviewed and updated as necessary;
- whether the board and senior management receive and review sufficient information to provide appropriate direction and control of insurance sales; and
- for retail insurance sales conducted through a networking arrangement with a third-party vendor, whether such arrangement is controlled by a written agreement that is approved by the bank's board of directors.

e. Privacy Rule Handbook

» A board-approved privacy policy is not required by the rule, but it can be an effective way to involve the board of directors in developing a privacy compliance strategy. A board-sanctioned privacy policy can be useful in communicating the bank's overall privacy commitment and strategy to the entire organization.

D. CFPB GUIDANCE

1. Supervisory Highlights: Summer 2013

» **BOARD OF DIRECTORS AND MANAGEMENT OVERSIGHT OF COMPLIANCE MANAGEMENT:**

- In a bank, the board of directors is ultimately responsible for developing and administering the compliance management system. In a nonbank offering consumer financial services, the ultimate responsibility may rest with a board of directors in the case of a corporate entity or with a controlling person, senior management, or some other body.
- An effective board of directors communicates clear expectations and adopts clear policy statements about consumer compliance, not only within the entity itself, but also to its service providers. The board should establish a compliance function within the entity, allocating sufficient resources to that function, commensurate with the entity's size, organizational complexity, and risk profile. The board should ensure that the compliance function is appropriately staffed with a qualified chief

compliance officer, and other additional compliance managers who have the authority and accountability necessary to implement the compliance management program, with clear and visible support from senior management, as well.

» **COMPLIANCE PROGRAM:**

- Management should develop, and the board should approve, a system of policies and procedures that address every consumer financial product or service offered by the entity. Policies and procedures should be formal, written documents that detail consumer compliance responsibilities and instruct employees on the appropriate methods for executing these responsibilities. Policies and procedures are expected to address compliance with all applicable Federal consumer financial laws in a manner designed to prevent violations and to detect and prevent associated risk of harm to consumers. Management and the board are expected to ensure that the policies and procedures are maintained and modified regularly to remain current and to serve as a reference for employees in their day-to-day activities.

- **TRAINING:**

  - *In addition to training employees, a compliance program should ensure that board members receive sufficient information, including training, to enable them to understand the entity's consumer compliance responsibilities and the commensurate resource requirements.*

- **MONITORING:**

  - *Management and the board should develop a system of risk-based periodic monitoring reviews in order to ensure that transactions and other consumer contacts are handled in accordance with Federal consumer financial laws and with the entity's own policies and procedures.*

» **INDEPENDENT COMPLIANCE AUDIT:**

- A compliance audit program provides a board of directors or its designated committees with a determination of whether policies and standards are being implemented to provide for the level of compliance and consumer protection established by the board. Audits should cover consumer sales as well as customer services. The audit results should be reported directly to the board or a board committee.

2. Supervisory Highlights: Fall 2012

» The CFPB's examiners have found that among the common features at financial institutions with well-developed fair lending compliance programs are regular fair lending training for all employees involved with any aspect of the institution's credit transactions, as well as all officers and board members, and meaningful oversight of fair lending compliance by management and where appropriate, the financial institution's board of directors.

3. CFPB Supervisory and Examination Manual 2.0 (October 2012).

» **COMPLIANCE MANAGEMENT REVIEW:** Examiners should seek to determine whether the board and senior management have:

- Demonstrated clear expectations about compliance, not only within the entity, but also to service providers.

- Adopted clear policy statements regarding consumer compliance.

- Appointed an appropriately qualified and experienced chief compliance officer and provided for other compliance officers with authority and accountability.

- Established a compliance function to set policies, proce-

dures, and standards.

- Allocated resources to the compliance function commensurate with the size and complexity of the entity's operations and practices, the Federal consumer financial laws and regulations to which the entity is subject, and necessary to avoid the potential consumer harm associated with violations of such laws and regulations.

- Addressed consumer compliance issues and associated risks of harm to consumers throughout product development and through the entity's handling of consumer complaints.

- Required audit coverage of compliance matters and reviewed the results of periodic compliance audits.

- Provided for recurring reports of compliance risks, issues, and resolution through a committee structure or to the board.

» HOME MORTGAGE DISCLOSURE ACT EXAMINATION PROCEDURES

- Examiners should evaluate whether the board of directors has established an independent review of the HMDA/Reg C policies and procedures, and HMDA data, to ensure compliance and accuracy, and is advised each year of the accuracy and timeliness of the financial institution's data submissions.

» TRUTH IN LENDING ACT EXAMINATION PROCEDURES

- Examiners should review compliance review and audit workpapers and determine whether significant deficiencies, and the root cause of the deficiencies, are included in reports to management/board.

» HOMEOWNERS PROTECTION ACT EXAMINATION PROCEDURES

- Examiners should review compliance review and audit workpapers and determine whether significant deficiencies, and the root cause of the deficiencies, are included in reports to management/board.

» FAIR CREDIT REPORTING ACT EXAMINATION PROCEDURES

- Examiners should review any compliance audit material, including workpapers and reports, to determine whether significant deficiencies and their causes are included in reports to management and/or the board of directors.

» TRUTH IN LENDING ACT EXAMINATION PROCEDURES (SEPT. 15, 2015)

- Examiners should review any compliance audit material, including workpapers and reports, to determine whether significant deficiencies and their causes are included in reports to management and/or the board of directors.

» ELECTRONIC FUND TRANSFER ACT AND REGULATION E EXAMINATION PROCEDURES (OCT. 30, 2015)

- Examiners should determine that the board and management have set clear expectations about compliance with Regulation E, not only within the entity but also concerning key business partners, including agents, correspondent banks, and software providers, to the extent relevant.

- Examiners should determine whether significant deficiencies and their causes are included in reports to management and/or to the board of directors or principal(s).

» EQUAL CREDIT OPPORTUNITY ACT EXAMINATION PROCEDURES (OCTOBER 30, 2015)

- Examination procedures include reviewing the process for the entity's board of directors (or a designated committee of the board, or principals if there is no board) and senior management to discuss fair lending issues and receive periodic updates on the entity's fair lending risks.

- Examination procedures include determining whether:

- *the entity's board of directors and senior management receive fair lending training;*
- *the entity communicates any training results or issues to the board and/or senior management;*
- *the entity provides periodic results of its fair lending monitoring and corrective action results to the board and/or senior management;*
- *the entity provides periodic fair lending complaints updates to the board and/or senior management;*
- *the entity's compliance audit program report to an audit committee or other committee of the board; and*
- *the entity provide periodic results of its fair lending related audits, and any resulting corrective actions, to the board and/or senior management.*

4. CFPB Bulletin 2014-01, Compliance Bulletin and Policy Guidance: Mortgage Servicing Transfers (August 19, 2014).

» CFPB expects all servicers under its jurisdiction, including those with significant transfer volume, to maintain a robust Compliance Management System (CMS). A robust CMS must, among other things, both ensure that violations of Federal consumer financial law do not occur during a transfer and must contain mechanisms for promptly identifying and remediating any violations of Federal consumer financial law that do occur. Entities with a robust CMS have strong policies and procedures, effective board oversight, and regular and properly directed training.

5. CFPB Bulletin 2013-02, Indirect Auto Lending and Compliance with the Equal Credit Opportunity Act

» To have a strong fair lending compliance program, there should be regular fair lending training for all employees involved with any aspect of the institution's credit transactions, as well as all officers and board members. (citing most recent Supervisory Highlights).

6. CFPB Bulletin 2012-07, Appeals of Supervisory Matters

» To initiate an appeal of adverse findings in a supervisory matter, the board of directors or principal(s) must authorize the appeal.

E. FFIEC/INTERAGENCY GUIDANCE

1. Booklets that Comprise the Federal Financial Institutions Examination Council Information Technology Examination Handbook[4]

The FFIEC's "Handbook Overview" presentation notes that "[a]lthough the booklets are intended for use by a wide range of audiences, the content is written at a level appropriate for a midlevel IT examiner. Examiners will target the workprogram procedures based on the risk in specific examination environments."

a. Audit Booklet

» The board of directors has overall responsibility for the effectiveness of the Information Technology ("IT") audit function.

» The board of directors and senior management are responsible for providing the audit function with sufficient resources to ensure adequate IT coverage and audit function independence.

» The board of directors and senior management are

4 Note: The guidance in this section applies to the Information Technology ("IT") policies, operations, programs, procedures and other IT related areas of banks, bank holding companies, thrifts, and credit unions.

responsible for ensuring that the institution's system of internal controls operates effectively.

» To meet its responsibility of providing an independent audit function with sufficient resources to ensure adequate IT coverage, the board of directors or its audit committee should:

  - Provide an internal audit function capable of evaluating IT controls;
  - Engage outside consultants or auditors to perform the internal audit function; or
  - Use a combination of both methods to ensure that the institution has received adequate IT audit coverage.

» An institution's board of directors may establish an "audit committee" to oversee audit functions and to report on audit matters periodically to the full board of directors.

» It is generally considered good practice for all institutions to use the requirements of the Sarbanes-Oxley Act of 2002 and 12 C.F.R. 363 as guidelines to ensure the independence of their audit committees.

» The board of directors should ensure that written guidelines for conducting IT audits have been adopted.

» The board of directors or its audit committee should assign responsibility for the internal audit function to a member of management who has sufficient audit expertise and is independent of the operations of the business.

» The board should give careful thought to the placement of the audit function in relation to the institution's management structure.

» The internal audit manager should report directly to the board of directors or its audit committee.

» The board or its audit committee is responsible for reviewing and approving audit strategies (including policies and programs), and monitoring the effectiveness of the audit function. The board or its audit committee should be aware of, and understand, significant risks and control issues associated with the institution's operations, including risks in new products emerging technologies, information systems, and electronic banking.

» The board or its audit committee members should seek training to fill any gaps in their knowledge related to IT risks and controls. The board of directors or its audit committee should periodically meet with both internal and external auditors to discuss audit work performed and conclusions reached on IT systems and controls.

» The board and management should involve the audit department in the development process for major new IT applications. The board and management should develop criteria for determining those projects that need audit involvement.

» The board should ensure that the audit department does not participate in activities that may compromise, or appear to compromise, its independence. These activities may include preparing reports or records, developing procedures, or performing other operational duties normally reviewed by auditors.

» For an effective program, the board should give the auditor the authority to:

  - Access all records and staff necessary to conduct the audit, and
  - Require management to respond formally, and in a timely manner, to significant adverse audit findings by taking appropriate corrective action.

» Internal auditors should discuss their findings and recommendations periodically with the audit committee or board of directors.

» The internal audit manager should report directly to the board of directors or to the audit committee regarding both audit issues and administrative matters. Alternatively, an institution may establish a dual reporting relationship where the internal audit manager reports to the audit committee or board for audit matters and to institution executive management for administrative matters.

» The board or its audit committee should determine the internal audit manager's performance evaluations and compensation.

» If internal expertise is inadequate, the board should consider using qualified external sources such as management consultants, independent auditors, or other professionals to supplement or perform the institutions internal audit function.

» The board of directors should establish an effective risk-based audit function.

» A successful risk-based IT audit program can be based on an effective scoring system. In establishing a scoring system, the board of directors and management should ensure the system is understandable, considers all relevant risk factors, and, to the extent possible, avoids subjectivity.

» Written guidelines on the use of risk assessment tools and risk factors developed by auditors should be reviewed with the audit committee of the board of directors.

» The board of directors of an institution that outsources its internal IT audit function should ensure that the structure, scope, and management of the outsourcing arrangement provides for an adequate evaluation of the system of internal controls.

» The board of directors of an institution remains responsible for ensuring that the outsourced internal audit function operates effectively and complies with all regulations governing such arrangements.

» Directors and senior management should ensure that the outsourced internal audit function is competently managed.

b. Business Continuity Planning Booklet

» A financial institution's board and senior management are responsible for overseeing the business continuity planning ("BCP") process, which includes:

- Establishing policy by determining how the institution will manage and control identified risks;
- Allocating knowledgeable personnel and sufficient financial resources to implement the BCP;
- Ensuring that the BCP is independently reviewed and approved at least annually;
- Ensuring employees are trained and aware of their roles in the implementation of the BCP;
- Ensuring the BCP is regularly tested on an enterprise-wide basis;
- Reviewing the BCP testing program and test results on a regular basis; and
- Ensuring the BCP is continually updated to reflect the current operating environment.

» It is the responsibility of an institution's board and senior management to ensure that the institution identifies, assesses, prioritizes, manages, and controls risks as park of the business continuity planning process. The board and senior management should establish policies that define how the institution will manage and control the risks that were identified. Once policy

is established, it is also important for the board and senior management to understand the consequences of these identified risks and support continuity planning on a continuous basis.

» The board and senior management should review and approve the BCP, with the frequency based on significant policy revisions resulting from changes in the operating environment, lessons learned from BCP testing, and audit and examination recommendations.

» The board should ensure that enterprise wide BCP tests are conducted at least annually, or more frequently depending on changes in the operating environment. Formal procedures should be established for reporting the implementation of the testing program and test results to the board and senior management.

» The Business Impact Analysis, which should be incorporated into and tested as part of the BCP, should be reviewed by the board and senior management periodically and updated to reflect significant changes in business operations, audit recommendations, and lessons learned during the testing process.

» The board should receive and review BCP audit reports addressing the effectiveness of the institution's process for identifying and correcting areas of weakness, and audit recommendations should be monitored to ensure that they are implemented in a timely manner.

» The board should review the BCP and test program at least annually.

» The board of directors is responsible for overseeing the development of the pandemic plan. The board or a committee thereof should also approve the institution's written plan and ensure that senior management is investing sufficient resources into planning, monitoring, and testing the final plan.

- Important risk management steps also include reviewing and approving the pandemic plan by the board or a committee thereof and senior management at least annually.

» The board of directors and senior management are responsible for properly overseeing outsourced relationships.

c. Development and Acquisition Booklet

» The board, or board designated committee, should formally approve technology project management methodologies (*e.g.*, the systems development life cycle methodology or an alternative methodology for managing products, including software development, or hardware, software, or service acquisition projects).

» Examiners will assess the level of oversight and support provided by the board and management relating to development, acquisition, and maintenance activities, including with respect to (among other things) the frequency and quality of technology-related board reporting; the commitment of the board and senior management to promote new products; and the level and quality of board-approved project standards and procedures.

» Examiners will evaluate organizational responsibilities to ensure the board and management:

- Clearly define and appropriately assign responsibilities;
- Appropriately assign security, audit, and quality assurance personnel to technology-related projects;
- Establish appropriate segregation-of-duty or compensating controls; and
- Establish appropriate project, technology committee, and board reporting requirements.

d. E-Banking Booklet

» A financial institution's board and management should understand the risks associated with e-banking services and evaluate the resulting risk management costs against the potential return on investment prior to offering e-banking services.

» The board of directors and senior management are responsible for developing the institution's e-banking business strategy, which should include:

- The rationale and strategy for offering e-banking services including informational, transactional, or e-commerce support;
- A cost-benefit analysis, risk assessment, and due diligence process for evaluating e-banking processing alternatives including third-party providers;
- Goals and expectations that management can use to measure the e-banking strategy's effectiveness; and
- Accountability for the development and maintenance of risk management policies and controls to manage e-banking risks and for the audit of e-banking activities.

» The board should approve an e-banking strategy that considers factors such as customer demand, competition, expertise, implementation expense, maintenance costs, and capital support.

» Once an institution implements its e-banking strategy, the board and management should periodically evaluate the strategy's effectiveness.

» The board and senior management must provide effective oversight of third-party vendors providing e-banking services and support. Effective oversight requires that institutions ensure the following practices are in place:

- Effective due diligence in the selection of new service providers that considers financial condition, experience, expertise, technological compatibility, and customer satisfaction;
- Written contracts with specific provisions protecting the privacy and security of an institution's data, the institution's ownership of the data, the right to audit security and controls, and the ability to monitor the quality of service, limit the institution's potential liability for acts of the service provider, and terminate the contract;
- Appropriate processes to monitor vendors' ongoing performance, service quality, security controls, financial condition, and contract compliance; and
- Monitoring reports and expectations including incidence response and notification.

» In order to comply with the USA PATRIOT Act and federal regulations, the board of directors must approve a customer identification program ("CIP"). The CIP must be written, incorporated into the institution's Bank Secrecy Act/Anti-Money Laundering Program.

» The board should review, approve, and monitor e-banking technology-related projects that may have significant impact on the financial institution's risk profile.

» The board should ensure appropriate programs are in place to oversee security, recovery, and third-party providers of critical e-banking products and services.

e. Information Security Booklet

» Financial institutions should implement an ongoing security process and institute appropriate governance for the security function, assigning clear and appropriate roles and responsibilities to the board of directors, management, and employees.

» The board of directors should approve the institution's plan to mitigate risk that integrates technology, policies, procedures, and training, otherwise known as the Information Security Strategy.

» The board of directors, or an appropriate committee of the board, is responsible for overseeing the development, implementation, and maintenance of the institution's information security program, and making senior management accountable for its actions. Oversight requires the board to provide management with guidance; approve information security plans, policies and programs; and review reports on the effectiveness of the information security program. The board should provide management with its expectations and requirements and hold management accountable for:

- Central oversight and coordination,
- Assignment of responsibility,
- Risk assessment and measurement,
- Monitoring and testing,
- Reporting, and
- Acceptable residual risk.

» The board should approve written information security policies and the written report on the effectiveness of the information security program at least annually. A written report to the board should describe the overall status of the information security program. At a minimum, the report should address the results of the risk assessment process; risk management and control decisions; service provider arrangements; results of security monitoring and testing; security breaches or violations and management's responses; and recommendations for changes to the information security program. The annual approval should consider the results of management assessments and reviews, internal and external audit activity related to information security, third-party reviews of the information security program and information security measures, and other internal or external reviews designed to assess the adequacy of information security controls.

» To ensure appropriate segregation of duties, the information security officers should report directly to the board or to senior management.

f. Management Booklet

» Financial institution boards of directors should oversee, while senior management should implement, a governance structure that includes the following:

- Effective IT governance;
- Appropriate oversight of IT activities;
- Comprehensive IT management, including the various roles played by management; and
- Effective enterprise architecture.

» The board of directors sets the tone and direction for an institution's use of IT. The board should approve the IT strategic plan, information security program, and other IT-related policies. To carry out their responsibilities, board members should understand IT activities and risks. The board or a board committee should perform the following:

- Review and approve an IT strategic plan that aligns with the overall business strategy and includes an information security strategy to protect the institution from ongoing and emerging threats, including those related to cybersecurity.
    - *The Information Security Standards require management to develop, and the board to approve, an infor-*

mation security program to protect the security and confidentiality of customer information. The board should also annually review a written report, prepared by management, regarding the financial institution's actions toward GLBA compliance.

- Promote effective IT governance.
- Oversee processes for approving the institution's third-party providers, including the third parties' financial condition, business resilience, and IT security posture .
- Oversee and receive updates on major IT projects, IT budgets, IT priorities, and overall IT performance. The board of directors may need to approve critical projects and activities, such as expanding the institution's product line to include mobile financial services.
- Oversee the adequacy and allocation of IT resources for funding and personnel.
- Approve policies to escalate and report significant security incidents to the board of directors, steering committee, government agencies, and law enforcement, as appropriate.
- Hold management accountable for identifying, measuring, and mitigating IT risks.
- Provide for independent, comprehensive, and effective audit coverage of IT controls.

» The board may delegate the design, implementation, and monitoring of specific IT activities to management or a committee (e.g., IT steering committee). The board remains responsible for overseeing IT activities and should provide a credible challenge to management.

- An IT steering committee generally comprises senior management and staff from the IT department and other business units. The steering committee typically is responsible for reporting to the board on the status of IT activities. The reports enable the board to make decisions without having to be involved in routine activities.

» In the event that executive management is unable to implement an objective or agree on a course of action, executive management should escalate that matter to the board for more guidance.

» The chief information security officer ("CISO") should report directly to the board, a board committee, or senior management and not IT operations management. The CISO typical responsibilities include implementing the information security strategy and objectives, as approved by the board of directors, including strategies to monitor and address current and emerging risks.

» The board should approve policies, while senior management should establish and implement policies, procedures, and responsibilities for the enterprise-wide business continuity program. The board should annually approve the institution's business continuity program. Management should also provide to the board on an annual basis a written report on the overall status of the business continuity program and the results of testing of the plan and backup systems.

» Financial institution boards should oversee, while senior management should implement, an IT planning process with the following elements

- Long-term goals and the allocation of IT resources to achieve them, usually within a three- to five-year horizon.
- Alignment of the IT strategic plan with the enterprise-wide business plan.
- Identification and measurement of risk before changes or new investment in technology are made.
- An IT infrastructure to support current and planned business operations.

- Integration of IT spending into the budgeting process and weighing of direct and indirect benefits against the total cost of ownership of the technology.

» A sound IT plan should involve the board of directors, senior management, and staff in the planning process. The board of directors should provide a credible challenge to management when the board reviews and approves the plan.

» The board should assess management's operational plans and its success in defining and meeting budgetary goals as one means of evaluating management's performance.

» The board should actively and effectively provide oversight of incentive compensation programs for IT management to ensure that the programs appropriately balance risk and reward and are compatible with effective controls and risk management. The board and senior management should consider appropriate succession and transition strategies for key managers and staff members.

» The audit department should send IT audit reports to appropriate management and directly to the board of directors or a designated board committee. The board of directors is responsible for overseeing the IT auditors' performance and compensation, including whether the IT auditors have the necessary expertise and the audit coverage is adequate, timely, and independent.

- Depending on the institution's size and complexity, the board of directors may completely outsource the IT audit function. In those cases, the outsourced auditor should be engaged by the board or audit committee.

» Once management has acquired appropriate insurance coverage, it customarily establishes procedures to review and ensure the adequacy of the coverage, including an annual program review by the board of directors.

» The board of directors should hold senior management responsible for ensuring appropriate oversight of third-party relationships.

g. Operations Booklet

» A financial institution's board of directors and senior management are responsible for overseeing a safe and sound IT operating environment that supports the institution's goals and objectives. The institution's responsibilities apply to centralized and decentralized operations centers, including those located within lines of business; functional operations; affiliates under the enterprise umbrella; and outsourcing arrangements. Key elements of these responsibilities include:

- Implementing an IT operational organization structure suitable to supporting the business activities of the institution;

- Documenting the systems in place, and understanding how these systems support the associated business processes;

- Establishing and supporting an appropriate control environment through risk identification, assessment, management, and monitoring;

- Creating a physically and logically secure operating environment;

- Providing for operational continuity and resiliency;

- Providing for adequate staffing and personnel selection, succession, and training; and

- Using qualified consultants and external auditors, when necessary.

» The board and senior management are responsible for understanding the risks associated with existing and

planned IT operations, determining the risk tolerance of the institution, and establishing and monitoring policies for risk management.

» The board and senior management are responsible for strategic technology planning, which is critical to effective IT governance.

» The board should approve IT governing policies that provide broad guidance in addressing risk tolerance and management. Policies should address key areas such as personnel, capital investment, physical and logical security, change management, strategic planning, and business continuity.

» The board of directors and management should enact IT policies and procedures sufficient to address and mitigate the risk exposure of their institutions.

h. Outsourcing Technology Services Booklet

» Before considering the outsourcing of significant functions, an institution's directors and senior management should ensure such actions are consistent with their strategic plans and should evaluate proposals against well-developed acceptance criteria.

» An effective outsourcing oversight program should provide the framework for management to identify, measure, monitor, and control the risks associated with outsourcing. The board and senior management should develop and implement enterprise-wide policies to govern the outsourcing process consistently.

- These policies should address outsourced relationships from an end-to-end perspective, including establishing servicing requirements and strategies; selecting a provider; negotiating the contract; and monitoring, changing, and discontinuing the outsourced relationship.

» The board and senior management should be aware of the risks associated with outsourcing agreements in order to ensure effective risk management practices.

» Institutions involved in outsourcing arrangements should monitor the financial condition of their service providers on an on-going basis. Once the financial review is complete, management should report the results to the board of directors or to a designated committee.

» Regardless of whether an institution's information processing is internal or outsourced, the financial institution's board of directors should ensure adequate audit coverage.

i. Retail Payment Systems Booklet

» Financial institutions engaged in retail payment systems should establish an appropriate risk management process that identifies, measures, and limits risks. Management and the board should manage and mitigate the identified risks through effective internal and external audit, physical and logical information security, business continuity planning, vendor management, operational controls, and legal measures.

- The board of directors is responsible for Payment System Risk policy compliance and should ensure management establishes sound internal operating practices, including compliance with applicable banking laws and carefully managing retail payment system-related financial risks. At a minimum, a financial institution's board of directors should:

- Understand the financial institution's practices and controls regarding the risks of processing large-dollar transactions for both its own account and the accounts of its customers or respondents;

- Establish prudent limits on the daylight overdraft or net debit position that the financial institution may incur in its Federal Reserve Bank reserve account or private-sector clearing and settlement systems; and

- Review periodically the institution's daylight overdraft activity to ensure the institution operates within the established guidelines.

» The board of directors should ensure an information technology audit program is in place and designed to test retail payment system internal controls and management policies and procedures.

» Retail payment systems contain confidential customer information subject to GLBA section 501(b) security guidelines. The board and management are responsible for protecting the confidentiality, integrity, and availability of these systems and data.

j. Supervision of Technology Service Providers

» A financial institution's use of a technology service provider to provide needed products and services does not diminish the responsibility of the institution's board of directors and management to ensure that these activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations.

- Examiners will assess the level and quality of oversight and support of the IT activities by the board of directors and management, including with respect to systems development and acquisition activities.

» Effective internal and external audit programs are also a critical defense against fraud and provide vital information to the board of directors about the effectiveness of internal controls systems.

- Examiners will assess the adequacy of the organization's overall IT audit program, including the internal and external audit's abilities to detect and report significant risks to management and the board of directors on a timely basis.

k. Wholesale Payment Systems Booklet

» Financial institutions require efficient systems for transferring funds internally, among themselves, and with their customers for large-dollar payments relating to financial market transactions and settling corporate and consumer payments. Management and the board should:

- Establish dual controls and separation of duties for funds transfer systems;

- Monitor and log access to funds transfer systems, maintaining an audit trail of all sequential transactions; and

- Incorporate the funds transfer controls into the organization's information security program to ensure the integrity and confidentiality of customer information.

» Financial institutions engaged in wholesale payment systems and related activities should establish appropriate risk management processes that identify, measure, and limit risks. Financial institutions should tailor their risk management processes based on the nature and complexity of their wholesale payments business and their participation in wholesale payment, clearance, and settlement systems. Management and the board of directors should manage and mitigate identified risks through effective and appropriate policies, procedures, and controls.

» Financial institutions should develop and provide for the continued administration of a program reasonably designed to ensure and monitor compliance with the record keeping and reporting requirements set forth in subchapter II of the Bank Secrecy Act. The Bank Secrecy Act requires a written compliance program that is approved by the board of directors. The board must note the approval in the board minutes. The compliance program must include, at a minimum:

- Provision for a system of internal controls to ensure ongoing compliance;

- Provision for independent testing for compliance to be conducted by institution personnel or by an outside party;

- Designation of an individual or individuals responsible for coordinating and monitoring day-to-day compliance; and
- Provision for training for appropriate personnel.

2. Bank Secrecy Act/Anti-Money Laundering Examination Manual (2014)

The Introduction to this Manual states that it "provides guidance to examiners for carrying out BSA/AML and Office of Foreign Assets Control (OFAC) examinations." The Introduction further notes that "[i]n order to effectively apply resources and ensure compliance with BSA requirements, the [M]anual is structured to allow examiners to tailor the BSA/AML examination scope and procedures to the specific risk profile of the banking organization."

» The board is responsible for creating an appropriate oversight culture that is consistent with sound risk management and control environment. The board should have well developed goals which target the client base in terms of minimum net worth, investable assets and types of products and services sought.

- The board is expected to be actively involved in establishing control and risk management goals for private banking activities, including effective audit and compliance reviews and should review relationship manager compensation reports, budget or target comparison reports and risk management reports.

» The board, acting through senior management, is responsible for ensuring that the bank maintains an effective BSA/AML internal control structure, including suspicious activity monitoring and reporting. The board should be informed of the compliance initiatives, compliance deficiencies, SARs filed and corrective action taken.

» The BSA training program should reinforce the importance that the board and senior management place on the bank's compliance with the BSA and ensure that all employees understand their role in maintaining an effective BSA/AML compliance program.

» A Customer Identification Program must be incorporated into the bank's BSA/AML compliance program, subject to approval by the bank's board of directors.

3. Additional Interagency Guidance

a. Interagency Statement on Prudential Risk Management for Commercial Real Estate Lending (12/18/2015)

» The statement notes that in general, financial institutions that succeeded during difficult economic cycles took actions including the following, which are consistent with supervisory expectations:

- established adequate and appropriate loan policies, underwriting standards, credit risk management practices, and concentration limits that were approved by the board or a designated committee;
- provided their boards and management with information to assess whether the lending strategy and policies continued to be appropriate in light of changes in market conditions; and
- maintained management information systems that provided the board and management with sufficient information to identify, measure, monitor, and manage concentration risk.

b. FFIEC Consumer Compliance Risk Management Guidance (12/11/2013)

» Components of a risk management program with regard to social media should include, among other things:

- a governance structure with clear roles and responsibilities whereby the board of directors or senior management direct how using social media contributes to the strategic goals of the institution and establish controls and ongoing assessment of risk in social media activities; and

- parameters for providing appropriate reporting to the financial institution's board of directors or senior management that enable periodic evaluation of the effectiveness of the social media program and whether the program is achieving its stated objectives.

c. Interagency Guidance on Leveraged Lending (3/21/2013)

» The board of directors should approve the institution's risk appetite with regard to leveraged lending based on the effect of leveraged lending on the overall risk profile, and the possible effect on earnings, liquidity and capital.

» The board should receive from senior management a summary of the bank's leveraged lending portfolio at least quarterly and timely reports on leveraged lending risks.

» The board must establish written procedures to handle the institution's pipeline management and establish a procedure for pipeline transactions that have not been sold according to their original distribution plan.

d. Supplemental Policy Statement on the Internal Audit Function and its Outsourcing (1/23/2013)

» The audit committee of an institution's board of directors should approve the internal audit charter that describes the purpose, authority, and responsibility of the internal audit function.

» In addition to ensuring that the institution has an effective system of internal controls, the board of directors and senior management are responsible for ensuring that internal controls are operating effectively.

» An institution's audit committee is responsible for establishing an appropriate internal audit function and ensuring that it operates adequately and effectively. The audit committee should be confident that the internal audit function addresses the risks and meets the demands posed by the institution's current and planned activities. Moreover, the audit committee is expected to retain oversight responsibility for any aspects of the internal audit function that are outsourced to a third party.

» The audit committee should provide oversight to the internal audit function. Audit committee meetings should be on a frequency that facilitates this oversight and generally should be held four times a year at a minimum, with additional meetings held by audit committees of larger financial institutions. Annually, the audit committee should review and approve internal audit's charter, budget and staffing levels, and the audit plan and overall risk-assessment methodology. The committee approves the chief audit executive's hiring, annual performance evaluation, and compensation.

» The audit committee and its chairperson should have ongoing interaction with the chief audit executive separate from formally scheduled meetings to remain current on any internal audit department, organizational, or industry concerns. In addition, the audit committee should have executive sessions with the chief audit executive without members of senior management present as needed.

» The audit committee should receive appropriate levels of management information to fulfill its oversight responsibilities.

» For further details, *see* Interagency Policy Statement on the Internal Audit Function and its Outsourcing described below.

e. Interagency Supervisory Guidance on Counterparty Credit Risk Management (6/29/2011)

» This guidance is especially intended for banks with large derivatives portfolios.

» The board of directors or a designated board-level committee (board) should clearly articulate the banking organization's risk tolerance for counterparty credit risk ("CCR") by approving relevant policies, including a framework for establishing limits on individual counterparty exposures and concentrations of exposures.

» Banking organizations should report counterparty exposures to the board and senior management at a frequency commensurate with the materiality of exposures and the complexity of transactions.

» The board and senior management should clearly delineate the respective roles of business lines versus risk management, both in terms of initiating transactions that have CCR, and of ongoing CCR management. The board and senior management should ensure that the risk management functions have adequate resources, are fully independent from CCR related trading operations (in both activity and reporting), and have sufficient authority to enforce policies and to escalate issues to senior management and the board (independent of the business line).

» The board should direct internal audit to regularly assess the adequacy of the CCR management framework as part of the regular audit plan. The board should review annual reports from internal audit and model validation or review, assessing the findings and confirming that management has taken appropriate corrective actions.

» The board should be apprised of summary model validation results, especially unresolved deficiencies.

f. Interagency Guidance on Implementation Issues Related to the Advanced Measurement Approaches for Operational Risk (7/20/2011)

» The advanced approaches rule requires a bank to have an internal audit function independent of business-line management that at least annually assesses the effectiveness of the controls supporting the bank's advanced systems and reports its findings to the bank's board of directors (or a committee thereof). Such controls include a bank's validation processes. As a practical matter, there may be overlap between a bank's validation and audit activities.

g. Interagency Appraisal and Evaluation Guidelines (12/10/2010)

» An institution's board of directors or its designated committee is responsible for adopting and reviewing policies and procedures that establish an effective real estate appraisal and evaluation program. The program should:

- Provide for the independence of the persons ordering, performing, and reviewing appraisals or evaluations.
- Establish selection criteria and procedures to evaluate and monitor the ongoing performance of appraisers and persons who perform evaluations.
- Ensure that appraisals comply with the Agencies' appraisal regulations and are consistent with supervisory guidance.
- Ensure that appraisals and evaluations contain sufficient information to support the credit decision.
- Maintain criteria for the content and appropriate use of evaluations consistent with safe and sound banking practices.
- Provide for the receipt and review of the appraisal or

evaluation report in a timely manner to facilitate the credit decision.

- Develop criteria to assess whether an existing appraisal or evaluation may be used to support a subsequent transaction.
- Implement internal controls that promote compliance with these program standards, including those related to monitoring third party arrangements.
- Establish criteria for monitoring collateral values.
- Establish criteria for obtaining appraisals or evaluations for transactions that are not otherwise covered by the appraisal requirements of the Agencies' appraisal regulations.

h. Underwriting Standards for Small Business Loans Originated Under the Small Business Lending Fund Program (12/2010)

» The board of directors of each institution participating in the Small Business Lending Fund program should ensure that its small business lending policy is consistent with safe and sound credit practices and supportive of the institution's participation in the program.

i. Interagency Guidance on Sound Incentive Compensation Policies (6/30/2010)

» The board of directors of a banking organization should directly approve the incentive compensation arrangements for senior executives. The board also should approve and document any material exceptions or adjustments to the incentive compensation arrangements established for senior executives and should carefully consider and monitor the effects of any approved exceptions or adjustments on the balance of the arrangement, the risk-taking incentives of the senior executive, and the safety and soundness of the organization.

» The board of directors of an organization also is ultimately responsible for ensuring that the organization's incentive compensation arrangements for all covered employees are appropriately balanced and do not jeopardize the safety and soundness of the organization. The involvement of the board of directors in oversight of the organization's overall incentive compensation program should be scaled appropriately to the scope and prevalence of the organization's incentive compensation arrangements.

» The board of directors of a large banking organization or other banking organization that uses incentive compensation to a significant extent should actively oversee the development and operation of the organization's incentive compensation policies, systems, and related control processes.

- The board of directors of such an organization should review and approve the overall goals and purposes of the organization's incentive compensation system. In addition, the board should provide clear direction to management to ensure that the goals and policies it establishes are carried out in a manner that achieves balance and is consistent with safety and soundness.
- The board of directors of such an organization also should ensure that steps are taken so that the incentive compensation system—including performance measures and targets—is designed and operated in a manner that will achieve balance.

» The board of directors should monitor the performance, and regularly review the design and function, of incentive compensation arrangements.

- The board of directors of a banking organization should closely monitor incentive compensation payments to senior executives and the sensitivity of those payments to risk outcomes. In addition, if the compensation arrangement for a senior executive includes a clawback provision, then the review should include sufficient

information to determine if the provision has been triggered and executed as planned.

- The board of directors of a banking organization should seek to stay abreast of significant emerging changes in compensation plan mechanisms and incentives in the marketplace as well as developments in academic research and regulatory advice regarding incentive compensation policies.
    - *However, the board should recognize that organizations, activities, and practices within the industry are not identical. Incentive compensation arrangements at one organization may not be suitable for use at another organization because of differences in the risks, controls, structure, and management among organizations.*
    - *The board of directors of each organization is responsible for ensuring that the incentive compensation arrangements for its organization do not encourage employees to take risks that are beyond the organization's ability to manage effectively, regardless of the practices employed by other organizations.*
- The board of a large banking organization or other organization that uses incentive compensation to a significant extent should receive and review, on an annual or more frequent basis, an assessment by management, with appropriate input from risk-management personnel, of the effectiveness of the design and operation of the organization's incentive compensation system in providing risk-taking incentives that are consistent with the organization's safety and soundness.
- Boards of directors of these organizations also should consider periodically obtaining and reviewing simulation analysis of compensation on a forward-looking basis based on a range of performance levels, risk outcomes, and the amount of risks taken.

» The organization, composition, and resources of the board of directors should permit effective oversight of incentive compensation.

- The board of directors of a banking organization should have, or have access to, a level of expertise and experience in risk-management and compensation practices in the financial services industry that is appropriate for the nature, scope, and complexity of the organization's activities.
    - *This level of expertise may be present collectively among the members of the board, may come from formal training or from experience in addressing these issues, including as a director, or may be obtained through advice received from outside counsel, consultants, or other experts with expertise in incentive compensation and risk-management.*
    - *The board of directors of an organization with less complex and extensive incentive compensation arrangements may not find it necessary or appropriate to require special board expertise or to retain and use outside experts in this area.*
- In selecting and using outside parties, the board of directors should give due attention to potential conflicts of interest arising from other dealings of the parties with the organization or for other reasons.
    - *The board also should exercise caution to avoid allowing outside parties to obtain undue levels of influence. While the retention and use of outside parties may be helpful, the board retains ultimate responsibility for ensuring that the organization's incentive compensation arrangements are consistent with safety and soundness.*
- If a separate compensation committee is not already in place or required by other authorities, the board of directors of a large banking organization or other banking organization that uses incentive compensation to a significant extent should consider establishing such a committee— reporting to the full board—that has primary responsibility for overseeing the organization's

incentive compensation systems.

- *A compensation committee should be composed solely or predominantly of non-executive directors. If the board does not have such a compensation committee, the board should take other steps to ensure that non-executive directors of the board are actively involved in the oversight of incentive compensation systems*

j. Interagency Guidance on Correspondent Concentration Risk (4/30/2010)

» Procedures on monitoring correspondent relationships should specify when relationships that meet or exceed internal criteria are to be brought to the attention of the board of directors or the appropriate management committee.

k. Interagency Policy Statement on Funding and Liquidity Risk Management (3/17/2010)

» The board of directors is ultimately responsible for the liquidity risk assumed by the institution. As a result, the board should ensure that the institution's liquidity risk tolerance is established and communicated in such a manner that all levels of management clearly understand the institution's approach to managing the trade-offs between liquidity risk and short-term profits.

» The board of directors or its delegated committee of board members should oversee the establishment and approval of liquidity management strategies, policies and procedures, and review them at least annually. In addition, the board should ensure that it:

- Understands the nature of the liquidity risks of its institution and periodically reviews information necessary to maintain this understanding.
  - *In normal business environments, senior managers should receive liquidity risk reports at least monthly, while the board of directors should receive liquidity risk reports at least quarterly.*
  - *Liquidity risk reports should impart to senior management and the board a clear understanding of the institution's liquidity risk exposure, compliance with risk limits, consistency between management's strategies and tactics, and consistency between these strategies and the board's expressed risk tolerance.*
- Establishes executive-level lines of authority and responsibility for managing the institution's liquidity risk.
- Enforces management's duties to identify, measure, monitor, and control liquidity risk.
- Understands and periodically reviews the institution's CFPs for handling potential adverse liquidity events.
- Understands the liquidity risk profiles of important subsidiaries and affiliates as appropriate.

l. Interagency Advisory on Interest Rate Risk Management (1/6/2010)

» The board of directors has the ultimate responsibility for the risks undertaken by an institution – including IRR. The board should understand and be regularly informed about the level and trend of their institutions' IRR exposure. The board or its delegated committee of board members should oversee the establishment, approval, implementation and annual review of IRR management strategies, policies, procedures and limits (or risk tolerances).

» An institution's IRR tolerance should be communicated so that the board of directors and senior management clearly understand the institution's risk tolerance limits and approach to managing the impact of IRR on

earnings and capital adequacy. IRR reports distributed to senior management and the board should provide aggregate information and supporting detail that is sufficient to enable them to assess the sensitivity of the institution to changes in market rates and important assumptions underlying the metrics used.

m. FFIEC – Risk Management of Remote Deposit Capture (1/14/2009)

» The board of directors or management should approve plans, policies, and significant expenditures and should review periodic performance and risk management reports on the implementation and ongoing operation of RDC systems and services. The board and senior management are ultimately responsible for safe and sound operations, including RDC products and services.

n. Interagency Statement on Pandemic Planning (12/18/2007)

» An institution's board of directors is responsible for overseeing the development of the pandemic plan.

» The board or a committee thereof should also approve the institution's written plan and ensure that senior management is investing sufficient resources into planning, monitoring, and testing the final plan.

» Board or a committee thereof and senior management review and approve the pandemic plan at least annually.

o. Interagency Policy Statement on the Allowance for Loan and Lease Losses (ALLL) (12/13/2006):

» The board is responsible for overseeing management's significant judgments and estimates pertaining to the determination of an appropriate ALLL. The board's oversight includes:

- reviewing and approving the institution's ALLL policies and procedures at least annually;
- reviewing management's assessment and justification that the loan review system is sound and appropriate for the size and complexity of the institution;
- reviewing management's assessment and justification for the amounts estimated and reported each period for the provision for loan and lease losses and the ALLL; and
- requiring management to periodically validate and, when appropriate, revise the ALLL methodology.

» Each institution should have a written policy that is reviewed and approved at least annually by the board of directors to evidence its support of and commitment to maintaining an effective loan review system.

- The loan review policy should address the following elements: the qualifications and independence of loan review personnel; the frequency, scope and depth of reviews; the review of findings and follow-up; and workpaper and report distribution.

p. Interagency Guidance on Concentrations in Commercial Real Estate (CRE) Lending, Sound Risk Management Practices (12/12/2006):

» The board of directors has ultimate responsibility for the level of risk assumed by the institution. The board of directors or a designated committee thereof should:

- Establish policy guidelines and approve an overall CRE lending strategy regarding the level and nature of CRE exposures acceptable to the institution, including any specific commitments to particular borrowers or prop-

erty types, such as multifamily housing.

- Ensure that management implements procedures and controls to effectively adhere to and monitor compliance with the institution's lending policies and strategies.
    - *When an institution does permit an exception, it should document how the transaction does not conform to the institution's policy or underwriting standards, obtain appropriate management approvals, and provide reports to the board of directors or designated committee detailing the number, nature, justifications, and trends for exceptions.*
- Review information that identifies and quantifies the nature and level of risk presented by CRE concentrations, including reports that describe changes in CRE market conditions in which the institution lends.
- Periodically review and approve CRE risk exposure limits and appropriate sublimits (for example, by nature of concentration) to conform to any changes in the institution's strategies and to respond to changes in market conditions.

q. Interagency Statement on Sound Practices Concerning Elevated Risk Complex Finance Activities (5/16/2006):

» The board and senior management should strive to create a firm-wide corporate culture that is sensitive to ethical or legal issues as well as the potential risks to the financial institution that may arise from unethical or illegal behavior. A financial institution's policies and procedures should provide for the appropriate levels of management and the board of directors to receive sufficient information and reports concerning the institution's elevated risk complex finance activities to perform their oversight functions.

r. Interagency Credit Risk Management Guidance for Home Equity Lending (5/16/2006):

» The agencies' real estate lending standards regulations require that an institution's real estate lending policies be consistent with safe and sound banking practices and that an institution's board of directors review and approve these policies at least annually.

» As the portfolio approaches concentration limits, the institution should analyze the situation sufficiently to enable the institution's board of directors and senior management to make a well-informed decision to either raise concentration limits or pursue a different course of action.

» Financial institutions should accurately track the volume of HLTV loans, including HLTV home equity and residential mortgages, and report the aggregate of such loans to the institution's board of directors.

- All real estate secured loans in excess of supervisory LTV limits should be aggregated and reported quarterly to the institution's board of directors.

s. Interagency Advisory on the Unsafe and Unsound Use of Limitation of Liability Provisions in External Audit Engagement Letters (2/9/2006):

» The federal banking agencies encourage boards of directors, audit committees, and management to closely review all of the provisions in the audit engagement letter before agreeing to sign. They should also be aware that certain insurance policies (such as error and omission policies and director and officer liability policies) might not cover losses arising from claims that are precluded by limitation of liability provisions. They should not enter into any agreement that incorporates limitation of liability provisions with respect to engagements for financial statement audits, audits of internal

control over financial reporting, and attestations on management's assessment of internal control over financial reporting.

t. Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies (1/20/2006):

» The board should be notified when SARs are filed. The board or a committee must satisfy specific requirements designed to ensure that the institution's information security program is developed, implemented and maintained under the supervision of those who are ultimately responsible. The board or a committee must approve the written information security program at the outset. The board or a committee must oversee the implementation and maintenance of the program thereafter, including assigning specific responsibility for implementing the program and reviewing management reports.

u. Interagency Guidelines Establishing Information Security Standards (12/2005)

» The board, or appropriate committee, must approve the written information security program. Thereafter, the board or appropriate committee must oversee the implementation and maintenance of the program. These duties include assigning specific responsibility for implementing the program and reviewing reports prepared by management.

v. Credit Risk Management Guidance for Home Equity Lending (5/16/2005)

» An institution's board of directors is required to review and approve at least annually real estate lending policies that are consistent with safe and sound banking practices.

w. Interagency Interpretive Guidance on the Provision of Banking Services to Money Services Businesses Operating in the United States (4/26/2005):

» The board should approve standards and guidelines on whether or not to close a bank account once a SAR has been filed.

x. Interagency Statement on the Purchase and Risk Management of Life Insurance (12/7/2004)

» Although the board may delegate decision-making authority related to purchases of bank-owned life insurance ("BOLI") to senior management, the board remains ultimately responsible for ensuring that the purchase and holding of BOLI is consistent with safe and sound banking practices.

y. Interagency Guidance on Establishing Accounts for Foreign Governments, Embassies and Political Figures (6/15/2004)

» As it would with any new account, an institution should evaluate whether or not to accept a new account for a foreign government, embassy or political figure. That decision should be made by the institution's management, under standards and guidelines established by the board of directors, and should be based on the institution's own business objectives, its assessment of the risks associated with particular accounts or lines of business, and its capacity to manage those risks.

z. Interagency Paper on Sound Practices To Strengthen the Resilience of the U.S. Financial System (4/11/2003)

» Boards of directors should review business continuity

strategies to ensure that plans are consistent with the firm's overall business objectives, risk management strategies, and financial resources.

aa. Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing (3/17/2003)

» The board of directors and senior management are responsible for having an effective system of internal control and an effective internal audit function in place at their institution. They are also responsible for ensuring that the importance of internal control is understood and respected throughout the institution. This overall responsibility cannot be delegated to anyone else. They may, however, delegate the design, implementation and monitoring of specific internal controls to lower-level management and the testing and assessment of internal controls to others.

» Accordingly, directors and senior management should have reasonable assurance that the system of internal control prevents or detects significant inaccurate, incomplete, or unauthorized transactions; deficiencies in the safeguarding of assets; unreliable financial reporting (which includes regulatory reporting); and deviations from laws, regulations, and the institution's policies.

» Directors should be confident that the internal audit function addresses the risks and meets the demands posed by the institution's current and planned activities. To accomplish this objective, directors should consider whether their institution's internal audit activities are conducted in accordance with professional standards, such as the IIA Standards for the Professional Practice of Internal Auditing.

» Directors and senior management should ensure that the following matters are reflected in their institution's internal audit function.

- **STRUCTURE.**
  - *The internal audit function should be positioned so that the board has confidence that the internal audit function will perform its duties with impartiality and not be unduly influenced by managers of day-to-day operations.*
    - The audit committee, using objective criteria it has established, should oversee the internal audit function and evaluate its performance.
    - The audit committee should assign responsibility for the internal audit function to a member of management (hereafter referred to as the manager of internal audit or internal audit manager) who understands the function and has no responsibility for operating the system of internal control.
  - *Under a dual reporting relationship (in which the manager of internal audit is functionally accountable to the audit committee on issues discovered by the internal audit function, while reporting to another senior manager on administrative matters), the board should consider the potential for diminished objectivity on the part of the internal audit manager with respect to audits concerning the executive to whom he or she reports.*
  - *In structuring the reporting hierarchy, the board should weigh the risk of diminished independence against the benefit of reduced administrative burden in adopting a dual reporting organizational structure. The audit committee should document its consideration of this risk and mitigating controls. The IIA Practice Advisory 1110-2: Chief Audit Executive Reporting Lines provides additional guidance regarding functional and administrative reporting lines.*
- **SCOPE.** At least annually, the audit committee should review and approve internal audit's control risk assessment and the scope of the audit plan, including how much the manager relies on the work of an outsourcing vendor. It should also periodically review internal audit's adherence to the audit plan. The audit committee

should consider requests for expansion of basic internal audit work when significant issues arise or when significant changes occur in the institution's environment, structure, activities, risk exposures, or systems.

- **COMMUNICATION.**
  - *To properly carry out their responsibility for internal control, directors and senior management should foster forthright communications and critical examination of issues to better understand the importance and severity of internal control weaknesses identified by the internal auditor and operating management's solutions to these weaknesses.*
  - *In periodic meetings with management and the manager of internal audit, the audit committee should assess whether management is expeditiously resolving internal control weaknesses and other exceptions. Moreover, the audit committee should give the manager of internal audit the opportunity to discuss his or her findings without management being present.*
  - *Furthermore, each audit committee should establish and maintain procedures for employees of their institution to submit confidentially and anonymously concerns to the committee about questionable accounting, internal accounting control, or auditing matters. In addition, the audit committee should set up procedures for the timely investigation of complaints received and the retention for a reasonable time period of documentation concerning the complaint and its subsequent resolution.*

» Even when outsourcing vendors provide internal audit services, the board of directors and senior management of an institution are responsible for ensuring that both the system of internal control and the internal audit function operate effectively.

» In any outsourced internal audit arrangement, the institution's board of directors and senior management must maintain ownership of the internal audit function and provide active oversight of outsourced activities.

» Management and the board of directors are expected to use reasonable standards, such as the IIA *Standards for the Professional Practice of Internal Auditing*, when assessing the performance of internal audit.

bb. Interagency Advisory on Mortgage Banking (2/25/2003)

» An institution's board of directors should establish limits on investments in mortgage-banking assets and evaluate and monitor such investment concentrations (on the basis of both asset and capital levels) on a regular basis.

» Given the sensitivity of the mortgage-servicing assets valuation to changes in assumptions and valuation policy, any such changes should be reviewed and approved by management and, where appropriate, by the board of directors.

» Board and management should ensure that internal audit staff possesses the necessary qualifications and expertise to review mortgage-banking activities or obtain assistance from qualified external sources.

cc. Interagency Advisory on the Unsafe and Unsound Use of Covenants Tied to Supervisory Actions in Securitization Documents (5/23/2002)

» Banking organization management and boards of directors should ensure that covenants related to supervisory actions or thresholds are not included in securitization documents.

dd. Joint Agency Statement on Parallel-Owned Banking Organizations (4/23/2002)

» U.S. depository institution's board of directors and senior management are expected to be cognizant of

the risks associated with being part of a parallel-owned banking structure, especially with respect to diversion of depository institution resources, conflicts of interest, and affiliate transactions.

ee. Policy Statement on Allowance for Loan and Lease Losses Methodologies and Documentation for Banks and Savings Institutions (7/2/2001)

» Boards of directors of banks and savings institutions are responsible for ensuring that their institutions have controls in place to consistently determine the allowance for loan and lease losses (ALLL) in accordance with the institutions' stated policies and procedures, generally accepted accounting principles (GAAP), and ALLL supervisory guidance.

» To fulfill this responsibility, boards of directors instruct management to develop and maintain an appropriate, systematic, and consistently applied process to determine the amounts of the ALLL and provisions for loan losses.

» Regardless of who develops and implements these policies, procedures, and underlying controls, the board of directors should assure themselves that the policies specifically address the institution's unique goals, systems, risk profile, personnel, and other resources before approving them.

» The amounts reported each period for the provision for loan and lease losses and the ALLL should be reviewed and approved by the board of directors.

» To ensure the methodology remains appropriate for the institution, the board of directors should have the methodology periodically validated and, if appropriate, revised.

» The audit committee should oversee and monitor the internal controls over the ALLL determination process.

» The board of directors should review and approve a summary of the amount to be reported in the financial statements for the ALLL.

» Management usually supports the validation process with the workpapers from the ALLL review function. Additional documentation often includes the summary findings of the independent reviewer. The institution's board of directors, or its designee, reviews the findings and acknowledges its review in its meeting minutes.

ff. Expanded Guidance for Subprime Lending Programs (1/31/2001)

» The board of directors and management are expected to ensure that the institution's process for determining an adequate level for the ALLL is based on a comprehensive and adequately documented analysis of all significant factors.

gg. FFIEC – Risk Management of Outsourced Technology Services (11/28/2000)

» The board of directors and senior management are responsible for understanding the risks associated with outsourcing arrangements for technology services and ensuring that effective risk management practices are in place.

» As part of this responsibility, the board and management should assess how the outsourcing arrangement will support the institution's objectives and strategic plans and how the service provider's relationship will be managed.

» The board of directors and management are responsible for ensuring adequate risk mitigation practices are in place for effective oversight and management of outsourcing relationships.

hh. Interagency Guidance on Asset Securitization Activities (12/13/1999)

» Audit or internal review staffs periodically review data integrity, model algorithms, key underlying assumptions, and the appropriateness of the valuation and modeling process for the securitized assets retained by the institution. The findings of such reviews should be reported directly to the board or an appropriate board committee.

- The interagency guidance provides additional guidance on reports to be reported to the board, or to "management and the board," including with respect to static pool cash collection analysis (to be provided to management and the board); sensitivity analysis with respect to default rates, prepayment or payment rates, and discount rates (to be provided periodically to the board); and periodic audit reviews of securitization activities, including transaction testing and verification (to be reported to the board or an appropriate board committee).

» The board and management are accountable for the "model builders" possessing the necessary expertise and technical proficiency to perform the modeling process.

» It is the responsibility of an institution's board of directors to ensure that its audit staff or independent review function is competent regarding securitization activities

» The Agencies expect an institution's board of directors and management to develop and implement policies that limit the amount of retained interests that may be carried as a percentage of total equity capital, based on the results of their valuation and modeling processes.

ii. Interagency Policy Statement on External Audits of Banks With Less Than $500 Million in Total Assets (9/1999)

» The board of directors of an institution is responsible for determining how to best obtain reasonable assurance that the institution's financial statements and regulatory reports are reliably prepared. In this regard, the board is also responsible for ensuring that its external auditing program is appropriate for the institution and adequately addresses the financial reporting aspects of the significant risk areas and any other areas of concern of the institution's business.

» The agencies encourage the board of directors of each institution that is not otherwise required to do so to establish an audit committee consisting entirely of outside directors However, if this is impracticable, the board should organize the audit committee so that outside directors constitute a majority of the membership.

» The audit committee or board of directors is responsible for identifying at least annually the risk areas of the institution's activities and assessing the extent of external auditing involvement needed over each area. The audit committee or board is then responsible for determining what type of external auditing program will best meet the institution's needs.

» When evaluating the institution's external auditing needs, the board or audit committee should consider the size of the institution and the nature, scope, and complexity of its operations. It should also consider the potential benefits of an audit of the institution's financial statements or an examination of the institution's internal control structure over financial reporting, or both.

- In addition, the board or audit committee may determine that additional or specific external auditing procedures are warranted for a particular year or several years to cover areas of particularly high risk or special concern. The reasons supporting these decisions should be recorded in the committee's or board's minutes.

» If, in its annual consideration of the institution's external

auditing program, the board or audit committee determines, after considering its inherent limitations, that an agreed-upon procedures/state-required examination is sufficient, they should also consider whether an independent public accountant should perform the work.

» When the external auditing program includes an audit of the financial statements, the board or audit committee obtains an opinion from the independent public accountant stating whether the financial statements are presented fairly, in all material respects, in accordance with generally accepted accounting principles (GAAP). When the external auditing program includes an examination of the internal control structure over financial reporting, the board or audit committee obtains an opinion from the independent public accountant stating whether the financial reporting process is subject to any material weaknesses.

» The board or audit committee of each institution at least annually should review the risks inherent in its particular activities to determine the scope of its external auditing program.

» The board of directors is expected to perform due diligence on the relevant experience and competence of the independent auditor and staff carrying out the work (whether or not an independent public accountant is engaged).

jj. Interagency Guidance on Subprime Lending (3/1/1999)

» Institutions that engage in subprime lending in any significant way should have board-approved policies and procedures, as well as internal controls that identify, measure, monitor, and control these additional risks.

» Prior to engaging in subprime lending, the board and management should ensure that proposed activities are consistent with the institution's overall business strategy and risk tolerances, and that all involved parties have properly acknowledged and addressed critical business risk issues.

» The board should ensure that staff possesses sufficient expertise to appropriately manage the risks in subprime lending and that staffing levels are adequate for the planned volume of subprime activity.

kk. Uniform Interagency Trust Rating System (12/23/1998)

» **MANAGEMENT.** The management rating is based upon an assessment of the capability and performance of management and the board of directors, including, but not limited to, the following evaluation factors:

- The level and quality of oversight and support of fiduciary activities by the board of directors and management, including committee structure and adequate documentation of committee actions.
- The ability of the board of directors and management, in their respective roles, to plan for, and respond to, risks that may arise from changing business conditions or the introduction of new activities or products.

» **EARNINGS.** The evaluation of earnings is based upon, but not limited to, an assessment of the following factors:

- The effectiveness of the institution's procedures for monitoring fiduciary activity income and expense relative to the size and scope of these activities and their relative importance to the institution, including the frequency and scope of profitability reviews and planning by the institution's board of directors or a committee thereof.

» **ALTERNATE RATING OF EARNINGS.** Alternate ratings are assigned based on the level of implementation of four

minimum standards by the board of directors and management. The standards include:

- Standard No. 3–The board of directors periodically determines that the continued offering of fiduciary services provides an essential service to the institution's customers or to the local community.

- Standard No. 4–The board of directors, or a committee thereof, reviews the justification for the institution to continue to offer fiduciary services even if the institution does not earn sufficient income to cover the expenses of providing those services.

ll. Interagency Policy Statement on Income Tax Allocation in a Holding Company Structure (11/23/1998)

» Tax allocation agreements between a holding company and its subsidiary institution(s) should be approved by the respective boards of directors.

mm. FFIEC Supervisory Policy Statement on Investment Securities and End-User Derivatives Activities (4/17/1998)

» The board of directors is responsible for approving major policies for conducting investment activities, including the establishment of risk limits.

- The board and senior management should review, at least annually, the appropriateness of its investment strategies, policies, procedures, and limits.

» The board should ensure that management has the requisite skills to manage the risks associated with such activities.

» To properly discharge its oversight responsibilities, the board should review portfolio activity and risk levels, and require management to demonstrate compliance with approved risk limits.

- Reports to the board of directors and senior management should summarize the risks related to the institution's investment activities and should address compliance with the investment policy's objectives, constraints, and legal requirements, including any exceptions to established policies, procedures, and limits.

- Institutions should provide reports to their boards on the market risk exposures of their investments on a regular basis.

» Boards should have an adequate understanding of investment activities. Boards that do not, should obtain professional advice to enhance its understanding of investment activity oversight, so as to enable it to meet its responsibilities under this policy statement.

- Especially with respect to the management of the credit risk of securities settlements, the agencies encourage the board of directors or a subcommittee chaired by a director to actively participate in the credit decision process.

    - *The agencies understand that institutions will have various approaches to the credit decision process, and therefore that the board of directors may delegate the authority for selecting dealers and establishing dealer limits to senior management.*

- The board may wish to adopt policies prohibiting employees who are directly involved in purchasing and selling securities for the institution from securities dealers from engaging in personal securities transactions with these same securities firms without specific prior board approval.

- The board may also wish to adopt a policy applicable to directors, officers, and employees restricting or prohibiting the receipt of gifts, gratuities, or travel expenses from approved securities dealer firms and their representatives.

nn. FFIEC's Revised Policy Statement on Corporate Business Resumption and Contingency Planning (7/14/1997)

» The board of directors and senior management of each financial institution is responsible for:

- Establishing policies and procedures, and assigning responsibilities to ensure that comprehensive corporate business resumption, contingency planning, and testing takes place.
- Annually reviewing the adequacy of the institution's business recovery and contingency plans and test results.
- Documenting such reviews and approvals in the board minutes.

oo. Interagency Statement on the Risks to Financial Institutions Involving Client/ Server Computer Systems (19/8/1996)

» It is the responsibility of the board of directors of financial institutions to develop and adopt appropriate policies, practices, or procedures covering management's responsibilities and controls for all areas of client/server computing activities.

pp. Joint Policy Statement on Interest Rate Risk (3/23/1996)

» The agencies expect that in implementing this guidance, bank boards of directors and senior managements will provide effective oversight and ensure that risks are adequately identified, measured, monitored and controlled.

» For its part, a bank's board of directors has two broad responsibilities:

- To establish and guide the bank's tolerance for interest rate risk, including approving relevant risk limits and other key policies, identifying lines of authority and responsibility for managing risk, and ensuring adequate resources are devoted to interest rate risk management.
- To monitor the bank's overall interest rate risk profile and ensure that the level of interest rate risk is maintained at prudent levels.

» The board and senior management should ensure that the structure of the bank's business and the level of interest rate risk it assumes are effectively managed and that appropriate policies and practices are established to control and limit risks. This includes delineating clear lines of responsibility and authority for the following areas:

- Identifying the potential interest rate risk arising from existing or new products or activities;
- Establishing and maintaining an interest rate risk measurement system;
- Formulating and executing strategies to manage interest rate risk exposures; and
- Authorizing policy exceptions.

» The board should approve policies that establish appropriate risk limits that reflect the board's risk tolerance.

» The senior management and the board or committee are expected to:

- Evaluate the level and trends of the bank's aggregated interest rate risk exposure.
- Evaluate the sensitivity and reasonableness of key assumptions – such as those dealing with changes in the shape of the yield curve or in the pace of anticipated loan prepayments or deposit withdrawals.
- Verify compliance with the board's established risk toler-

ance levels and limits and identify any policy exceptions.

- Determine whether the bank holds sufficient capital for the level of interest rate risk being taken.

qq. Interagency Statement on Retail Sales of Nondeposit Investment Products (2/24/1994)

» A depository institution involved in retail nondeposit investment product activities should adopt a written statement that addresses the risks associated with the sales program and contains a summary of policies and procedures outlining the features of the institution's program and addressing, at a minimum, the concerns described in the interagency policy statement.

» The institution's statement should be adopted and reviewed periodically by its board of directors.

» If a depository institution directly or indirectly, including through a subsidiary or service corporation, engages in activities under which a third party sells or recommends nondeposit investment products, the institution should, prior to entering into the arrangement, conduct an appropriate review of the third party. The institution should have a written agreement with the third party that is approved by the institution's board of directors.

» Findings of compliance reviews should be periodically reported directly to the institution's board of directors, or to a designated committee of the board.