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

Prepared for The Clearing House Association L.L.C.

by Reed Smith LLP

March 28, 2012

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

Title 12, United States Code[1]

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. 12 U.S.C. 626 (foreign banking).

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. 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, 629.

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.

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

[1] We note that the Dodd-Frank Wall Street Reform and Consumer Protection Act instituted some changes to U.S. Federal Securities laws. These changes would apply to publicly listed holding companies but are outside the scope of this document. For instance, The Securities and Exchange Act of 1934 (15 U.S.C. 78 et. seq.) was amended to add a new Section 10C. on Compensation Committees.

affiliate of the bank is a principal underwriter of the securities. 12 U.S.C. 371c-1 (section 23B of the Federal Reserve Act).

Authorization of the bank to contract for or purchase from any of its directors (or any firm of which any of the directors is a member) any securities or other property when the purchase is made in the regular course of business upon terms not less favorable to the bank than those offered to others. Authorize the bank to sell securities or other property to a director, or to a firm of which a director is a member, in the regular course of business on terms not more favorable to such director or firm than those offered to others. 12 U.S.C. 375.

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

Authorization of loan to executive that cause a statutorily-imposed aggregate credit limit to such executive to be exceeded, subject to certain conditions. Establish credit limits for executive officers more stringent that those set forth in statute. 12 U.S.C. 375b.

Each insured depository institutions shall have an independent audit committee entirely made up of outside directors who are independent of management of the institution, except as otherwise provided in statute. 12 U.S.C. 1831m(g)(1).

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). 12 U.S.C. 161 requires three directors' signatures.

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 the members of the board of directors who do not have an interest in the transaction. 12 U.S.C. § 1828(z).

Title 12, Code of Federal Regulations - OCC Regulations

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

Declaration of cash dividends and property dividends. 12 C.F.R. 5.66.

Reorganize as subsidiary of a bank holding company. 12 C.F.R. 5.32.

Increase the number of the bank's directors, subject to certain limits. 12 C.F.R. 7.2007

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 the board of directors. 12 C.F.R. 9.18.

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. Id.

The bank's board of directors must comply with the OCC regulation on minimum security devices and procedures, and ensure that a security program which equals or exceeds 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 shall 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 shall report at least annually to the bank's board of directors on the effectiveness of the security program. 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 by the bank's audit committee or board of directors;
- Establish and maintain prudent credit underwriting practices that, among other things, includes 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; and
- Provide periodic earnings reports with adequate information for management and the board of director to assess earnings performance.

According to 12 C.F.R. Part 30, Appendix B -- Interagency Guidelines Establishing Standards for Safeguarding Customer Information, the board of directors or an appropriate committee of the board of each bank shall (a) approve the bank's written information security program, and (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.

The bank's real estate lending policies must be reviewed and approved by the board of directors at least annually. 12 C.F.R. 34.62.

According to 12 C.F.R. Part 34 Appendix A to Subpart D -- Interagency Guidelines for Real Estate Lending:

- 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 (as defined in the Interagency Guidelines for Real Estate Lending).
- The bank must individually report exception loans of a significant size to its board of directors.

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. 34.84.

Pursuant to 12 C.F.R. 5.30(j), national banks must comply with 12 U.S.C. 1831r-1 which requires, among other things, that each depository institution adopt a policy on branch closings.

Title 12, Code of Federal Regulations - FDIC Regulations

Undercapitalized insured depository institutions 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. 303.201.

Board of directors must 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 insured depository institution to release examination report to a majority shareholder. 12 C.F.R. 309.6.

Board of directors of insured depository institutions must take certain action with respect to indemnification payments to institution-affiliated parties. 12 C.F.R. 359.0; 12 C.F.R. 359.5.

Securitization agreements covered by 12 C.F.R. 360.6 must be in writing, approved by the board of directors or its loan committee (as reflected in the minutes of a meeting of the board of directors or committee), and have been continuously, from the time of execution in the official record of the bank. 12 C.F.R. 360.6(c)(2).

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. 12 C.F.R. 363.5.

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. Id.

- 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 are:

  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.

- The board of directors may appoint other responsibilities to the audit committee.

Title 12, Code of Federal Regulations - Federal Reserve Board Regulations

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.

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. Id.

Various matters must be reported to or acted upon by a bank's board of directors under Federal Reserve Board Regulation O. 12 C.F.R. Part 215.

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.

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 must 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 or an appropriate committee of the board of each bank holding company shall approve the bank holding company's written information security program and oversee the development, implementation and maintenance of the bank holding company's program and review reports from management. Each bank holding company shall report at least annually to its board or an appropriate committee of the board with respect to the security program. Appendix F to 12 C.F.R. Part 225 - - Interagency Guidelines Establishing Standards for Safeguarding Customer Information.

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

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

Comptroller's Handbook - Internal and External Audits

Board of directors or its audit committee reviews and approves risk assessments or the aggregate result thereof and annual risk-based audit plans (that establish internal and external audit schedules, audit cycles, work program scope, and resource allocation for each area to be audited) at least annually.

The board of directors or its audit committee monitors the implementation of the audit program and its audit schedule. Board/Audit Committee reports should be prepared as part of the internal audit manager's regular (OCC recommends quarterly) reporting to and discussions with the audit committee.

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.
- 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.

The auditors should perform follow-up activities promptly and report the results to the board of directors or its audit committee.

The internal auditor or the manager (director) of internal audit should report directly and regularly to the board of directors. (Also, see OCC-2003-12 [3/17/2003].)

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.

The board of directors performs due diligence on the relevant experience and competence of the independent auditor and staff carrying out the requisite audit work.

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 our both jointly.

The internal auditor and board of directors must be assured that a vendor can acceptably complete the work to be outsourced.

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.

OCC examiners will determine if, as required by SEC regulations, an audit committee report is made which states whether the audit committee reviewed and discussed audited financial statements with management.

SEC regulations provide that a Proxy statement must state whether the board of directors has adopted a written charter for its audit committee.

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.

OCC Circulars, Bulletins Handbooks and Journals

A banks' derivatives activities should be approved by the bank's board of directors, a committee thereof or by appropriate senior management staff as designated by the board of directors. Any significant changes in the bank's derivatives activities should be approved by the board of directors, or by an appropriate level of senior management, as designated by the board. Appropriate governance by the board of directors should include an initial endorsement of significant policies (and changes, as applicable) and periodic approval thereafter, as appropriate considering the scope, size and complexity of the bank's derivatives activities. BC-277 (10/27/1993).

The bank's real estate lending policy must be reviewed and approved by the bank's board of directors at least annually. BC-265 (12/31/1992) (rescinded and incorporated into the OCC's real estate and construction lending handbook). The policies governing an institution's real estate lending activities must include prudent underwriting standards that are periodically reviewed by the board of directors. BB-91-43 (11/5/1991) (note - this document is not included on the OCC's current or rescinded banking bulletin list); EC-234(Rev) (3/20/1992) (rescinded and incorporated into the OCC's real estate lending handbook).

The board of directors or a board committee should approve and enforce bank policies to control foreign currency risk. BC-216 (9/11/1986).

The bank's investment policy is to be approved by the board of directors. The decision to purchase shares of an investment company is the ultimate responsibility of the board of directors. BC-220 (11/21/1986).

A bank may not enter into an repurchase agreement without obtaining control of the securities unless, among other things, the transaction is within credit limitations that have been pre-approved by the board of directors, or a committee of the board, for unsecured transactions with the counterparty. OCC 1998-06(2/19/1998).

Bank management must evaluate the adequacy of the Allowance for Loan and Lease Losses at least quarterly and report the findings to the board of directors before preparing the (Call Report). BC-201 (2/20/1992) (rescinded and incorporated into the OCC's ALLL Handbook).

The board of directors or audit committee of each bank should analyze the adequacy of external audit coverage in their bank. If it is determined that an external audit is not necessary, reasons supporting such an assessment should be included in board or committee minutes. BC-190 (3/18/1985); note: BC-190 is not included on OCC's lists of current or rescinded banking circulars.

The board of directors and senior management of financial institutions are responsible for: (a) establishing policies and procedures, and assigning responsibilities to ensure that comprehensive corporate business resumption, contingency planning, and testing takes place; (b) annually reviewing the adequacy of the institution's business recovery and contingency plans and test results; and (c) documenting such reviews and approvals in board minutes. OCC-2003-18(5/21/2003).

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. BC-58(Rev) (12/28/1983).

The scope of loan reviews by a bank's loan review personnel should be approved by the institution's board of directors on an annual basis or when any significant changes to the scope of

the reviews are made. A report that summarizes the results of the loan review should be submitted to the board of directors on at least a quarterly basis, or more frequently when material adverse trends are noted. BB-93-60 (12/21/1993) (rescinded and incorporated into OCC's ALLL Handbook).

With respect to the reduced documentation small business loan rules, the responsibility of the board of directors is to acknowledge the bank's participation in its meeting minutes and assign responsibility for maintaining sufficient records to comply with the program. BB-93-54 (11/2/1993).

OCC's evaluation of a bank's CRA performance will consider the degree of involvement of the bank's board of directors in various aspects of the bank's CRA efforts. BB-92-43 (8/10/1992) (rescinded and incorporated into Community Reinvestment Act Handbook).

Before a bank begins marketing gold or silver bullion, the board of directors should formally authorize the program and establish appropriate procedures and policies. BC-58 (11/3/1981).

A bank's assessment of its home loan practices for purposes of determining if the bank's lending shows disparate treatment on a prohibited basis should be reported to the bank's board of directors and recorded in the board's minutes. AL 91-7 (12/11/1991).

The interagency statement on retail nondeposit investment sales sets forth various board requirements; see OCC-94-13 (2/24/1994):

- When a bank uses a third party vendor to sell nondeposit investment products, the bank's board of directors must adopt a written policy addressing the scope of the activities of the third party, as well as the procedures the bank intends to use for monitoring the third party's compliance with the Interagency Statement. The bank should enter into a written agreement with the third party vendor that has been approved by the bank's board of directors. Periodic compliance reviews of this activity should be reported directly to the bank's board of directors or a committee of the board.

- Bank directors are responsible for evaluating the risks imposed by bank-related sales and are expected to adopt a program statement and self-regulatory policies and procedures to ensure compliance with all requirements. The institution's statement should be adopted and reviewed periodically by its board of directors …. Banks can establish independence of audit or compliance personnel if such personnel determine the scope, frequency, and depth of their own reviews; report their findings directly to the board of directors or an appropriate committee of the board; have their performance evaluated by persons independent of the investment product sales function; and receive compensation that is not connected to the success of investment product sales.

If a bank uses its own internal model to measure interest rate risk, the OCC will assess the model being used; the bank should periodically review and validate the model with results communicated and reviewed by management and the board of directors on at least a quarterly basis. OCC 95-46 (8/9/1995) (rescinded and incorporated into the OCC's Interest Rate Risk Handbook).

Effective board and senior management oversight of a bank's interest rate risk activities is the cornerstone of a sound risk management process. For its part, a bank's board of directors has two broad responsibilities: (a) 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; and (b) To monitor the bank's overall interest rate risk profile and ensure that the level of interest rate risk is maintained at prudent levels. OCC 96-36 (7/12/1996) (rescinded and incorporated into the OCC's Interest Rate Risk Handbook).

At a minimum, a risk management program for a credit card solicitation campaign 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. AL 96-7 (9/25/1996).

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. OCC 96-25 (4/30/1996).

A bank's board of directors should ensure that its 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 and management have established policies on such transactions that minimize risks posed by potential legal and conflict-of-interest issues. EC-245 (12/14/1988).

A bank's board must review the bank's policies and procedures on correspondent relationships annually (but need not approve individual correspondent relationships). When a bank relies on its bank holding company to select and monitor correspondents, or on a correspondent to choose other correspondents with which to place the depository institution's federal funds, the bank's board of directors must have reviewed and approved the selection criteria used. EB-93-6 (8/31/1993).

As the bank's established credit risk limits for portfolio management are approached, the risk management process should require that the board of directors and/or senior management review the portfolio to assess the reasons for the increased level of risk and to take appropriate action. The board of directors and senior management should ensure that risk control functions are independent of the lending function and are staffed adequately to perform their assigned duties. AL-97-3 (3/11/1997).

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 if the delegation is prudent; the board of directors, or its designee, should approve the delegation and ensure an agreement setting forth duties and responsibilities is in place. OCC-97-22 (5/15/1997).

Significant internal control deficiencies should be reported directly to the board of directors. OCC-2003-12(3/17/2003).

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 bank's board of directors should review, approve and monitor technology projects that may have a significant impact on the bank's earnings, operations or capital. Senior managers with knowledge of the bank's technology initiatives should report periodically to the board of directors on technology initiatives. OCC 98-3 (2/4/1998).

The OCC and other federal banking regulatory agencies recommend that the board of directors of each institution establish and maintain an external auditing program, and in connection therewith to establish an audit committee consisting entirely of outside directors. The audit committee of the board is responsible for reviewing and approving eternal audit program policies at least annually; it also should identify at least annually the risk areas of the institution's activities and assess the extent of external auditing involvement needed over each area. The audit committee should report its findings periodically to the board of directors. OCC 99-37 (10/7/1999).

The Interagency Guidance on Asset Securitization Activities provide that institutions engaged in securitizations should have an independent risk management function commensurate with the complexity and volume of their securitizations and their overall risk exposures. In carrying out the risk management function, management should periodically quantify and document the potential impact to both earnings and capital and report the results to the board of directors. 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. OCC 99-46 (12/14/1999).

Tax sharing agreements between a holding company and its subsidiary institutions should be approved by the respective boards of directors. OCC 98-56 (12/10/1998).

In addressing price risk management as a component of an institutions efforts to manage the risks associated with financial derivatives and bank trading activities, the OCC notes that while Value-at-risk (VaR) is the most common method dealer/trading banks use to measure aggregate price risk, a bank's board of directors must understand the method's limitations. OCC 99-2 (1/25/1999).

Before a bank engages in subprime lending, the board of directors must have done a comprehensive due diligence. OCC 99-15 (4/5/1999).

Bank management must evaluate the adequacy of its ALLL at least quarterly and report its findings to the board of directors before preparing the bank's call report. AL 97-8 (8/6/1997).

A bank's board of directors should be provided periodic reports, including compliance reports and audit reports, on the bank's payday lending activities. AL 2000-10 (11/27/2000).

In a joint statement on sound risk management practices for leveraged finance, the OCC (along with the other federal bank regulators) noted that higher risk credits, including leveraged finance transactions, require frequent monitoring by banking organizations, and that at least quarterly, management and the board of directors should receive comprehensive reports about the characteristics and trends in such exposures. Examiners are instructed to determine if management and the board of directors have established policies for leverage finance that minimize the risks posed by potential legal issues and conflicts of interest. OCC 2001-18 (4/9/2001).

Management should periodically review the reasonableness and accuracy of the major assumptions used in the bank's interest rate risk measurement systems . . . these major assumptions and their impact should be reviewed by the board of directors or a committee thereof on, at least, an annual basis. AL-95-1 (2/8/1995).

A bank's board of directors should consider any plan to engage in financial futures and forward placement markets and should endorse specific written policies and procedures in authorizing them; the policy shall include, among other things, the method of valuation to be employed. The board should also establish limitations applicable to futures, forward and standby contract

positions. BC-277 (10/27/1993) - note: BC-79 is not included on OCC's lists of current or rescinded banking circulars.

A bank may purchase an interest in a mutual fund comprised wholly of bank-eligible securities if, among other things, the bank's investment policy, as formally approved by the board of directors, specifically provides for such investments; prior approval of the board of directors is obtained for initial investments in specific funds and recorded in board minutes. BC-220 (11/21/1986).

In its policy statement on investment securities and end-user derivatives activities of April, 1998, the OCC encourages the board of directors or a subcommittee chaired by a director, to actively participate in the credit decision process; the board may delegate the authority for selecting dealers and establishing dealer limits to senior management. The board of directors is responsible for approving major policies for conducting investment activities, including the establishment of risk limits. 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. Boards should have an adequate understanding of investment activities. OCC 98-20 (4/27/1998).

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. Reporting should be frequent enough to provide timely and adequate information to judge the changing nature of the institution's risk profile and to evaluate compliance with stated policy objectives and constraints. Id.

The board of directors is responsible for supervision and oversight of investment portfolio and end-user derivatives activities, including the approval and periodic review of policies that govern relationships with securities dealers. Id.

The board and senior management should review, at least annually, the appropriateness of its investment strategies, policies, procedures, and limits. Id.

Institutions should provide reports to their boards on the market risk exposures of their investments on a regular basis. Id.

Board of directors must approve self-assessment of daylight overdraft cap. Federal Reserve Policy of Payments System Risk, as amended on 01/11/2007.

Policy Statement for ALLL Methodologies and Documentation for Banks and Savings Institutions (66 F.R. 35629 7/6/01)

At present, the financial institution's board of directors is responsible for approving ALLL policies and attesting to the validity of the regulatory reports that indicate the ALLL.

OCC Publication: Detecting *Red Flags in Board Reports - A Guide for Directors* (revised in 2004)

While not citing any specific authority, the guide states that as a general rule, boards of directors should regularly receive reports on (1) financial performance [comprised of capital, asset quality, earnings, liquidity, sensitivity to market risk, and growth], (2) credit portfolio management [specifically, loan quality, ALLL, and loan summary], (3) liquidity risk management, (4) interest rate risk management, (5) investment portfolio management [selection of security dealers,

categorization of securities, and investment reports], (6) financial derivatives and off-balance-sheet activities [financial derivatives, asset securitizations, credit commitments, and mortgage banking], (7) audits and internal control, (8) consumer compliance [special emphasis on fair lending, CRA, BSA], (9) asset management, (10) management information systems, (11) internet banking, and (12) the OCC's overall assessment [Uniform Ratings, RAS, Relationship of RAS to Uniform Ratings].

With respect to financial performance - capital, the guide states that financial reports the board should review are to focus on comparative financial statements (income statements for the month and year-to-date, which are compared with the budget and with results from prior years; balance sheets for the month and year-to-date, which compare balances in individual asset and liability categories with balances at the same date in the previous year and with projections, if appropriate), and key financial performance ratios (tier capital/adjusted average assets; tier 1 risk-based ratio and total risk-based ratio; cash dividends/net income; and equity growth rate versus asset growth rate).

When addressing financial performance - asset quality, the guide urges directors to 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/total loans and leases; noncurrent loans and leases/equity capital; ALLL/total loans and leases; ALLL/net loan and lease losses; noncurrent loans and leases/ALLL; net loan and lease losses/average loans and leases.

The guide advises directors that the level and trend of the following measures, compared with the bank's previous performance and the current performance of peer banks, are important in evaluating earnings: net income/average assets; net income/average total equity; net interest/average earning assets; noninterest income/average assets; overhead (noninterest) expense/average assets; provision expense/average assets.

Directors should regularly review the following liquidity leading indicators for signs of increasing liquidity risk: loan to deposit ratio; net noncore funding dependence; net short-term liabilities/total assets; on-hand liquidity/total liabilities; reliance on wholesale funding.

The guide explains that the following ratios can help directors evaluate a bank's sensitivity to changes in interest rates: long-term assets/total assets; nonmaturity deposits/long-term assets; residential real estate/total assets; asset depreciation/tier 1 capital.

Directors are advised to identify growth patterns by comparing historical and budgeted growth rates for assets, loans, volatile liabilities, core deposits, and income and expenses. Comparing the bank's growth rate with that of peers is also recommended.

In order to evaluate loan quality, directors are told to review the following reports: risk rating, problem loans, past due and nonaccrual loans, renegotiated and restructured loans, OREO, exception loans.

Directors are advised to review the following to determine whether the ALLL is adequate: management's quarterly evaluation of the adequacy of the ALLL; management's problem loan list; charge-off and recovery experience; a reconcilement of the ALLL for the current period and previous year-end; any independent analysis of ALLL.

Board members are told they can find out what types of loans the bank is making and management's lending practices by looking at lists of new credits approved, loans renewed, concentration of credit, and participations purchased and sold.

Directors are advised that the following reports can assist them in assessing the bank's liquidity risk: liquidity risk report; funds provider report; projected needs and sources; cash flow or funding gap report; funding concentration report; contingency funding plan.

The guides provide that reports to the board should measure the bank's current interest rate risk position relative to earnings at risk and capital at risk limits. The three most common risk measurement systems used to quantify a bank's interest rate risk exposure are gap reports, simulation models and economic value sensitivity models. Evidently, the OCC expects the board to receive and study the report or model used by the bank.

Directors are to review and approve a list of securities firms with whom the bank is authorized to do business; the directors must ensure that such dealers are financially stable, reputable and knowledgeable.

Directors 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 for all municipal and corporate securities; adjusted historic al cost for each security relative to its current market value; purchases and sales; sensitivity analysis of the value of the portfolio in different interest rate environments.

The following reports are characterized by the guide as helpful to directors in their efforts to assess financial derivatives activities: credit risk exposure; trends in derivatives usage; compliance with policies and risk limits; results of stress testing; impact on income from derivatives.

The guide explains that with respect to their monitoring of asset securitizations, directors and management should ensure that (a) independent risk management processes are in place to monitor securitization pool performance on an aggregate and individual transaction level; (b) 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; (c) 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 bank; (d) management maintains accurate and timely risk-based capital calculations; (e) internal limits are in place to govern maximum retained interests; (f) the bank has a realistic liquidity plan in place in case of market disruptions; (g) transactions that do not create recourse to the bank. In addition, the guide identifies 13 matters to be addressed by reports to the board on revolving transactions and installment loans.

The board is to receive reports from management projecting the funding sources for loan commitments and lines of credit. Directors should ensure that bank policy supports a loan officer's refusal to advance funds.

The board must consider whether a bank's control systems and auditing methods, records and procedures are appropriate.

A good practice is for accountants to disclose, in writing, all relationships with the bank and its related entities that could affect the accountant's objectivity in an audit, and to discuss their independence with the bank's audit committee.

The audit committee should require external auditors to submit engagement letters before commencing audit work.

Designated consumer compliance officers should have direct access to the board. The board should periodically receive formal reports on compliance matters.

An effective board places special emphasis on fair lending, CRA and BSA. Periodic self assessments can help the board determine the bank's progress toward achieving its internal CRA goals. Directors should ensure that the bank's BSA program includes proper internal controls, independent testing, and appropriate staff training and that it is updated whenever regulatory changes take place.

Boards of directors should expect to routinely see financial performance reports related to each of its asset management businesses. In this respect, the following reports were identified as helpful in assessing risks and financial performance of assets management activities: new business/loss business reports; investment reports; litigation reports; investment performance analyses; profitability/budget reports; fiduciary audit reports; trust bank capital and liquidity analysis reports.

The board should (a) review, approve and monitor internet banking technology-related projects, and (b) receive regular reports on the technologies employed, the risks assumed and how those risks are managed.

The board of directors is to review the report of examination to obtain the OCC's objective assessment of the bank.

Federal Reserve Board Bank Holding Company Supervision Manual

(References are to Manual Section Numbers)

2005 Note: As of October 31, 2005, the Manual makes 797 references to the term *directors*. This is an average of almost one reference to that term on every other page of the Manual.

Holding company inspection objectives include the following: To determine (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 (a) determining whether the board of directors of the parent company reviews the audit reports, regulatory examination reports, and board minutes of its subsidiaries, and (b) a review of 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)

Parent company management should have policies in place to prevent funding practices that put at risk the welfare of the subsidiary banks or the consolidated organization. The parent should be expected to maintain policies for itself and its subsidiaries that provide guidance and controls for funding practices. (2010.1)

The reporting with respect to asset/liability management should clearly indicate the current exposure and thus the potential for liquidity problems. (Id.)

Although the Federal Reserve Board did not directly apply its real estate lending standards regulation to bank holding companies and their nonblank subsidiaries, those entities are expected to conduct and to supervise real estate lending activities prudently, consistent with safe and sound lending standards. 2010.2.1.

Lending policies must be reviewed and approved by the institution's board of directors at least annually. Id.

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)

In supervising subsidiaries, a holding company is advised of the importance of integrating subsidiaries into a consolidated plan. In this respect, the planning should 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 term goals, intermediate term objectives and short term goals should be periodically reviewed, preferably annually, by the holding company's board of directors. 2010.4.

Holding company 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. 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. 2010.4.1. and 2010.4.2.

The interagency policy statement on the retail sale of nondeposit investment products 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.

An 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; such policies must be reviewed and approved by the institution's board of directors or its designated committee. 2010.12.1.

If a bank holding company has a split-dollar life insurance arrangement with its subsidiary, FRB examiners are told to determine 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. 2020.9.6.

The manager of internal audit should report directly to the board or directors or a committee thereof. …. Significant matters should be promptly reported directly to the board of directors or its audit committee and senior management. Directors and senior management should ensure that certain specified matters are reflected in their institution's internal audit function 2060.05.1.1.1. Also, see 2060.05.1.2.

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 determine if an audit program is annually reviewed and approved by the board of directors. 2060.1.4.4.

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 (2060.1.3), and (b) audit reports are submitted on a timely basis to the directors and senior management (2060.1.3); examiners should review the engagement letter between the board of directors and the outside auditor (Id.). The manual notes, however, that the primary thrust of the inspection should be directed toward the audit activities that relate to the parent company and all subsidiaries. An assessment of the audit function as it pertains to the bank(s) is primarily the responsibility of the regulatory agency that examines that particular bank. The examiner should review the latest bank examination reports to note comments and deficiencies cited concerning internal controls and the audit function. In addition to providing an input into the overall assessment of the audit function, review of the bank examination reports may provide a basis for determining areas of investigation during the inspection. (Id.)

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). Examiners are instructed to review the manner and frequency of presentations to the board of directors of the insurance coverage. (2060.5.8).

Little guidance is provided with respect to reports that are to go to a board of directors. Typical guidance on point is the direction to examiners that they are to determine if audit reports are submitted on a timely basis to directors and management. (2060.1.4). Similarly, holding companies are advised that they should "maintain policies and procedures that clearly outline the organization's risk management guidance for trading and derivative activities; such policies should identify the risk tolerances of the board of directors and should clearly delineate lines of authority and responsibility for managing these 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 . . . the board of directors should encourage discussions between its members and senior management, as well. (Id.)

The board of directors should review at least annually the appropriateness of its investment strategies, policies, procedures, and limits. (2126.1.1.4.1).

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. . . Reporting should be frequent enough to provide timely and adequate information to judge the changing nature of the institution's risk profile and to evaluate compliance with stated policy objectives and constraints. (2226.1.1.4.2.) The board of directors is responsible for supervision and oversight of investment portfolio and end-user derivatives activities, including the approval and periodic review of policies that govern relationships with securities dealers. (2126.1.1.5.2)

Inspection objectives with respect to securitization activities includes 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)

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) The board of directors and management is 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)

Inspection objectives with respect to an institution's futures, forward and option contract activities include the ascertainment of whether the banking organization's board of directors has established written limitations with respect to financial-contract positions. (Examiners are reminded that the holding company policy statement requires that the board of directors establish written policies and position limitations in connection with financial-contract positions.) in addition, examiners are to determine 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)

A banking organization's board of directors must adopt policies and procedures that establish effective real estate appraisal and evaluation programs. The board is expected to periodically review the appraisal policies and procedures that establish the appraisal and evaluation program for real estate lending. (2231.0.1; 2231.0.12)

With respect to investment or financial adviser activities, the manual states that the examiner should determine if the board of directors has developed adequate objectives and policies. (3130.1.3.2.1) In addition, the manual provides that if the board of directors does not directly supervise investment adviser activity, the examiner should determine if: (a) a responsible board committee(s) has been named to exercise the function; (b) the board's minutes reflect periodic but timely review of conduct and operating results of the function; (c) minutes of the board require and approve, where necessary, appropriate written policies, strategic plans, and management reports relating thereto; (d) the board or its committee(s) review(s) audit and regulatory reports, litigation developments, earnings and expense reports and changes to fee schedules; (e) the board, through adoption of formal policies and provisions for auditing, seek to ensure the integrity of the organization's records and operational systems; (f) the board or a board committee consider, periodically review, and provide for insurance protection. (3130.1.3.2.3.2)

The manual suggests that when an adviser uses options and/or futures, the board of directors or a directors' level committee must have approved a policy and strategy for their use. (3130.1.3.2.3.2)

In the section on securities underwriting and trading policies, the manual indicates that underwriting/trading policies should be established by the board of directors and should be reviewed at least quarterly by the board to determine their adequacy in light of changing conditions. In addition, the board should periodically review the activity to ensure compliance with its policies. (3240.0.13.1)

When addressing offsetting repurchase and resale transactions, the manual indicates that the board of directors should have adopted written policies for such transactions. (3240.0.13.2)

If a holding company has a futures commission merchant subsidiary, the FCM's board of directors should approve written policies summarizing the firm's activities, and addressing oversight by the board or a board designated committee. (3250.0.10.2)

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)

Whenever there is a consolidated income tax return filed, it is important that a formal tax agreement exists between the parent and each subsidiary, approved by each board of directors. (5010.35.3)

Manual Items Added by Supplement since June 2001

To better understand and manage the risk in leveraged-finance portfolios, the Board of Directors and senior management must ensure that credit-analysis processes are comprehensive, monitoring is frequent, and portfolio reports are detailed. 2010.2.3

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

The Board of Directors is expected to establish standards and guidelines regarding the acceptance of new accounts for a foreign government, embassy or political figure. 2010.13

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..3.1.2.1. The loan review function should report directly to the board of directors. 2065.3.1.5.2. The board of directors should approve the scope of loan reviews at least annually. Id. A report that summarizes the result of the loan review should be submitted to the board of directors on at least a quarterly basis. Id. The board of directors should be informed more frequently than quarterly when material adverse trends are noticed. Id.

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.

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.

With respect to asset securitizations, a 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.

Significant policies and procedures regarding credit-enhanced or asset-backed commercial paper should be approved and reviewed periodically by the board of directors. 2128.03.4.

Management and the board of directors should ensure that covenants relating to supervisory actions or thresholds are not included in securitization documents. 2128.05.

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.

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. 2178.0.1.

The board or a committee of the board should approve policies that identify authorized activities and managerial oversight and should articulate risk tolerance and exposure limits of FCM activities. 3250.0.2.1.

A financial holding company's board of directors should approve merchant banking portfolio objectives, overall investment strategies, and general investment policies that are consistent with the institution's financial condition, risk profile, and risk tolerance. 3909.0.2.1.

The board of directors should approve equity activities 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, start-ups, or seed financing), and appropriate diversification-related aspects of equity investments such as industry, sector, and geographic concentrations. Id.

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.

Compliance personnel should report findings of their compliance reviews of such programs directly to the board or board committee. 3950.0.4.1.4.

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. County exposure limits should be approved by the board of directors or a board committee. 4090.0.2.6.

Directors and senior management should have reasonable assurance that the system of internal audit prevents or detects 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 consider whether their institution's internal audit activities are conducted in accordance with professional standards, such as the Institute of Internal Auditors' *Standards for the Professional Practice of Internal Auditing*. 2060.05.1.1. (Policy Statement)

Significant matters should be promptly reported (by internal audit function) to the board of directors or its audit committee. 2060.05.1.1.4. (Policy Statement)

Directors and senior management must ensure that the outsourced internal audit function is competently managed. 2060.05.2.2.1. (Policy Statement)

Booklets that Comprise the Federal Financial Institutions Examination Council Information Technology Examination Handbook[2]

Audit Booklet

The board of directors has overall responsibility for the effectiveness of the Information Technology ("IT") audit function. (p. 2)

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. (p. 2)

The board of directors and senior management are responsible for ensuring that the institution's system of internal controls operates effectively. (p. 2)

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. (p.3)

The board of directors should review and approve IT polices, procedures and processes. (p. A-2)

The board should approve audit plans and schedules, reviews actual performance of plans and schedules, and approves major deviations to the plan. (p. A-2)
Internal auditors should discuss their findings and recommendations periodically with the audit committee or board of directors. (p.5)

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. (p. 3)

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. (p. 5)

For an effective program, the board should give the auditor the authority to:

- Access all records and staff necessary to conduct the audit, and

[2] 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.

- Require management to respond formally, and in a timely manner, to significant adverse audit findings by taking appropriate corrective action. (p. 5)

Internal auditors should discuss their findings and recommendations periodically with the audit committee or board of directors. (p. 5)

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. (p. 5)

The board or its audit committee should determine the internal audit manager's performance evaluations and compensation. (p. 5)

It is the responsibility of the audit committee and management to carefully consider the extent of auditing that will effectively monitor the internal control system subject to consideration of the internal audit function's costs and benefits. (p.5)

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. (p. 5-6)

The audit program should include a mission statement or audit charter outlining the purpose, objectives, organization, authorities, and responsibilities of the internal auditor, audit staff, audit management, and the audit committee. (p.6)

The audit committee should formally approve the audit plan annually, or review it annually in the case of multi-year audit plans. The internal auditors should report the status of planned versus actual audits, and any changes to the annual audit plan, to the audit committee for its approval on a periodic basis. (pp. 6-7)

If an audit rating system is implemented, it should be approved by the audit committee. (p.7).

The board of directors should establish an effective risk-based audit function. (p. 8)

Risk based IT audit programs should include board or audit committee approval of risk assessments and annual risk-based audit plans that establish audit schedules, audit cycles, work program scope, and resource allocation for each area audited. (p.9).

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 managements should ensure the system is understandable, considers all relevant risk factors, and, to the extent possible, avoids subjectivity. (p. 9)

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. (p. 10)

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. (p. 12)

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. (p. 12)

Directors and senior management should ensure that the outsourced internal audit function is competently managed. (p. 14)

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. (p. 2)

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. (p. 2)

As part of their support for continuity planning, the board and senior management should assign knowledgeable personnel and allocate sufficient financial resources to properly implement an enterprise-wide BCP. (p.2)

The board and senior management are also responsible for ensuring that the BCP is independently reviewed by the internal or external auditor at least annually. The board and senior management should also 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. (p. 3)

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. (p. 3)

To maintain the effectiveness of the BCP, the board and senior management 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. After the BCP is approved and tested, the board and senior management have an on-going responsibility to oversee critical business processes and ensure that the BCP is updated to reflect the current operating environment. (p. 3)

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. (p. 7)

The BCP should be reviewed and approved by the board and senior management at least annually. (p. 9).

While outsourcing BCP development may be a viable option, the board and management are ultimately responsible for implementing and maintaining a comprehensive BCP. (p.9)

The board and senior management are responsible for establishing and reviewing an enterprise wide testing program. (p. 12)

An enterprise-wide business continuity testing policy should be established by the board and senior management and should set expectations for business lines and support functions to follow in implementing testing strategies and test plans. The policy should establish a testing cycle that increases in scope and complexity over time. As such, the testing policy should continuously improve by adapting to changes in business conditions and supporting expanded integration testing. (p.13)

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. (p. 18)

The board should establish an on-going, process-oriented approach to business continuity planning that is appropriate for the size and complexity of the organization. This process should include a Business impact analysis (BIA), a risk assessment, risk management, and risk monitoring and testing. Overall, this planning process should encompass the organization's business continuity strategy, which is the ability to recover, resume, and maintain all critical business functions. (p. A-2)

The board and senior management should ensure that integral groups are involved in the business continuity process (e.g. business line management, risk management, IT, facilities management, and audit). (p. A-2)

The board and senior management should establish an enterprise-wide BCP and testing program that addresses and validates the continuity of the institution's mission critical operations. (p. A-2)

The board and senior management review and approve the BIA, risk assessment, written BCP, testing program, and testing results at least annually and document these reviews in the board minutes. (p. A-2)

The board and senior management oversee the timely revision of the BCP and testing program based on problems noted during testing and changes in business operations. (p. A-3)

The board or a committee thereof and senior management should provide appropriate oversight of the institution's pandemic preparedness program. (p. A-6)

Development and Acquisition Booklet

Financial institutions use various methods to manage technology projects. Organizations may employ a systems development life cycle model or alternative methodology when managing any project, including software development, or hardware, software, or service acquisition projects. Regardless of the method used, it should be tailored to match a project's characteristics and risks. The board, or board designated committee, should formally approve project methodologies. (p. 3)

E-Banking Booklet

While the institution does not have to manage the daily administration of the component systems of its e-banking system, its management and board remain responsible for the content, performance, and security of the e-banking system. (p.3)

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. (p. 14)

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. (p. 15)

The board should approve an e-banking strategy that considers factors such as customer demand, competition, expertise, implementation expense, maintenance costs, and capital support. (p. 16)

Once an institution implements its e-banking strategy, the board and management should periodically evaluate the strategy's effectiveness. (p. 17)

In evaluating the effectiveness of the institution's e-banking strategy, the board should also consider whether appropriate policies and procedures are in effect and whether risks are properly controlled. Unless the initial strategy establishes clear accountability for the development of policies and controls, the board will be unable to determine where and why breakdowns in the risk control process occurred. (p. 17)

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 vendor's ongoing performance, service quality, security controls, financial condition, and contract compliance; and
- Monitoring reports and expectations including incidence response and notification. (p. 18)

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. (p. 24)

The institution's board and management should ensure that internal control and audit processes are adequate to enable the identification, measurement, and monitoring of the risks associated with e-banking. Management should attempt to quantify increased expenses and losses due to internal control-related weaknesses and fraud. (p. A-2)

The financial institution should ensure it has the proper level of expertise to make business decisions regarding e-banking and network security. The board of directors and senior management may need to enhance their understanding of technology issues. If such expertise is not available in-house, the institution should consider engaging outside expertise. (p. A-2)

The board should review, approve, and monitor e-banking technology-related projects that may have significant impact on the financial institution's risk profile. (p. A-5)

The board should ensure appropriate programs are in place to oversee security, recovery, and third-party providers of critical e-banking products and services. (p. A-5)

FedLine Booklet

Verification refers to designated fields that must be re-keyed by a second operator. If the institution should decide to set the verification level, for the appropriate "Verify Thresholds," at any amount greater than $0.00, the board of directors should approve the amount and note their approval in the board minutes. (p. 16)

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. (p. 3)

The board of directors should approve the institutions plan to mitigate risk that integrates technology, policies, procedures, and training, otherwise known as the Information Security Strategy. (p. 3)

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. (pp. 4-5)

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. (p. 5)

To ensure appropriate segregation of duties, the information security officers should report directly to the board or to senior management. (p. 5)

Management Booklet

The board of directors and executive management should understand and take responsibility for IT management as a critical component of their overall corporate governance efforts. (p. 1)

The board should ensure a program exists to manage and monitor operational risk. This program should address the institution's tolerance for risk, the effectiveness of internal controls, management's accountability in regards to risk mitigation, and the processes needed to manage IT effectively. (p. 2)

Financial institution boards of directors and management should establish IT oversight by ensuring:

- Strong board involvement and awareness of IT activities;
- Circulation and enforcement of sound policies and procedures;
- Implementation and maintenance of an effective risk management process;
- Staff members are competent and sufficient to perform their mission;
- Effective Management Information Systems (MIS) are in place; and
- A sound project management structure is utilized. (p. 3)

The board of directors should approve IT plans, policies, and major expenditures. To carry out their responsibilities, board members should be familiar with information technology and data center concepts and activities. (p. 4)

If the board chooses to delegate their responsibility for monitoring IT activities to a senior management committee or IT steering committee:

- The committee should regularly report to the board on the status of major IT projects or issues;
- The committee should ensure the board has adequate information to make informed decisions about IT operations; and
- The board should define the responsibilities of the IT steering committee within a committee charter. (p.4)

The board is responsible for overseeing and approving the development, implementation, and maintenance of a comprehensive, written information security program, as required by the Gramm-Leach-Bliley Act. The information security program should include appropriate administrative, technical, and physical safeguards based on the size, complexity, nature and scope of the institutions operations. (p. 6)

The board may delegate information security monitoring to an independent audit function and information security officer. To ensure independence, the information security officer, if any, should report directly to the board or senior management. (p. 6)

To ensure independence, the information security officer should report directly to the board or senior management rather than through the IT department. (p.6)

The board and senior management should ensure cooperation between management and IT audit. Is should also ensure timely and accurate response to audit concerns and exceptions. The IT audit area should report directly to the board of directors or a designated committee of the board comprised of outside directors. The board is responsible for overseeing the audit department's performance and compensation. (p. 7)

The board should ensure IT auditors have the necessary expertise and that audit coverage is adequate, timely, and independent. (p. 7)

The board should define and enforce incentive programs for IT management, similar to those available for other senior management of the organization, to reward managers who meet IT performance goals. (p. 8)

The board and senior management should consider appropriate succession and transition strategies for key managers and personnel. (p. 9)

In the case of Management Information Systems, the board should ensure that a comprehensive internal and external audit program exists to ensure the adequacy of internal controls. (p. 10)

Financial institution boards and management should implement an IT planning process that:

- Aligns IT with the corporate wide strategic plan;
- Aligns IT strategically and operationally with business units;
- Maintains an IT infrastructure to support current and planned business operations;
- Integrates IT spending into the budgeting process and weighs direct and indirect benefits against the total cost of ownership of the technology; and
- Ensures the identification and assessment of risk before changes or new investment in technology. (p. 11)

The board must review and approve the IT plan. (p.11)

The board should oversee management's efforts to create and maintain an alignment between IT

and corporate-wide strategies by:

- Confirming IT strategic plans are aligned with the business strategy; Determining that IT performance supports the planned strategy;
- Ensuring the IT department is delivering on time, within budget, and to specification;
- Directing IT strategy to balance investments between systems that support current operations, and systems that transform operations and enable business lines to grow and compete in new areas; and
- Focusing IT resource decisions on specific objectives such as entry into new markets, enhanced competitive position, revenue growth, improved customer satisfaction, or customer retention. Board Briefing on IT Governance, 2nd Edition, IT Governance Institute, www.itgi.org, 2003. (pp. 12-13)

The board should assess management's plans and its success in defining and meeting budgetary goals as one means of evaluating the performance of the data processing and operations management. (pp. 13-14)

Management and the board should monitor risk mitigation activities to ensure identified objectives are complete or in process. Monitoring should be ongoing, and departments should provide progress reports to management on a periodic basis. (pp. 16-17)

Once management has acquired appropriate IT insurance coverage, the insurance program selected by management should be reviewed annually, at a minimum, by the board of directors. (p. 19)

The board of directors is responsible for overseeing the development, implementation, and maintenance of the institution's information security program. The board should provide management with guidance and review the effectiveness of management's actions. The board should approve written information security policies and the information security program at least annually. The board should provide management with its expectations and requirements for:

- Central oversight and coordination;
- Areas of responsibility;
- Risk measurement;
- Monitoring and testing;

- Reporting; and
- Acceptable residual risk. FFIEC IT Examination Handbook, Information Security Booklet (p.20)

The Board should also review an annual report, prepared by management, regarding the bank's actions toward GLBA compliance. (p.20).

The board of directors and senior management are responsible for establishing policies, procedures, and responsibilities for organization-wide business continuity planning. At a minimum, the board of directors should annually update and approve the institution's business continuity plans. Management should document, maintain, and test the organization's business continuity plan and back-up systems on a periodic basis to mitigate the risk of system failures and unauthorized intrusions. Management should also report the tests of the plan and back-up systems to the board of directors on an annual basis. (p.20)

The board and senior management should develop and implement enterprise-wide policies and procedures to govern the outsourcing process including establishing objectives and strategies, selecting a provider, negotiating the contract, and monitoring the outsourced relationship. (p. 23)

The board should:

- be directly involved in setting or managing IT oversight,
- establish a steering committee,
- implement processes and procedures that meet objectives of governing IT policies,
- approve appropriate oversight policies for Information Security,
- have current policies, processes and procedures that result in compliance with applicable regulatory requirements, e.g., GLBA,
- address risks regarding system development and acquisition, and
- have a process in place for business continuity planning. (pp. A-2-A-3)

The Board should establish:
- A defined and functioning role for either the CIO/CTO;
- Integration of business line manager(s) into the IT oversight process; and
- Involvement of front line management in the IT oversight process. (p. A-4)
- The Board of Directors and management should effectively report and monitor IT-related risks. (p. A-4)

Management and the Board of Directors should:
- Annually review and approve a formal, written, information security program,
- Approve and monitor the risk assessment process,
- Approve and monitor major IT projects,
- Approve standards and procedures,
- Monitor overall IT performance,
- Maintain an ongoing relationship between IT and business lines,
- Review and approve infrastructure, vendor, or other major IT capital expenditures based upon board set limits,
- Review and monitor the status of annual IT plans and budgets,

- Review management reports, measure actual performance of selected major projects against established plans. Determine the reasons for the shortfalls, if any, and
- Review the adequacy and allocation of IT resources, including staff and technology. (p. A-4)

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. (p. 2)

Senior management and the board of directors are responsible for ensuring IT operates in a safe, sound, and efficient manner throughout the institution. Because information systems-whether centralized or distributed-are tightly interconnected and highly interdependent, failure to adequately supervise any part of the IT environment can heighten potential risks for all elements of IT operations and the business as a whole. As a result, the board and senior management should coordinate IT controls throughout the institution's operating environment including all outsourcing and third-party arrangements.(pp. 2-3)

Although senior management and the board can delegate implementation and oversight of daily operations to information technology management, they have final responsibility for safe, sound, controlled, and efficient operations. (p. 3)

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. (p. 3)

The board and senior management are responsible for strategic technology planning, which is critical to effective IT governance. (p. 3)

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. (p. 11)

The board of directors and management should enact IT policies and procedures sufficient to address and mitigate the risk exposure of their institutions. (p. 11)

Outsourcing Technology Services Booklet

The financial institution's board and senior management should establish and approve risk based policies to govern the outsourcing process. The policies should recognize the risk to the institution from outsourcing relationships and should be appropriate to the size and complexity of the institution. (p.2)

Before considering the outsourcing of significant functions, an institutions directors and senior management should ensure such actions are consistent with their strategic plans and should evaluate proposals against well-developed acceptance criteria. (p. 2)

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. (p. 3)

The board and senior management should be aware of the risks associated with outsourcing agreements in order to ensure effective risk management practices. (p .3)

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. (p. 16)

Regardless of whether an institutions information processing is internal or outsourced, the financial institution's board of directors should ensure adequate audit coverage. (p. 17)

Retail Payment Systems Booklet

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. (p. 34)

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. (p. 41)

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. (p. 42)

Acquiring banks are ultimately responsible for any risks posed to the payment system by their sponsored merchants and third-party service providers. Management and the board of directors of all participants, including the acquiring banks, must have a clear understanding of the risk associated with acquiring activities and must understand their obligations under credit card association rules. (p.52)

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. (p. 1)

Wholesale Payment Systems Booklet

Management and the board of directors should oversee the implementation of the risk management strategy, policies, and controls through appropriate governance arrangements, effective external and internal audits, and appropriate management information systems. (p.16)

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. (p. 11)

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. (pp. 21-22)