WHAT'S NEW IN THIS REVISED SECTION

Effective January 2015, footnote 2 was revised to include a reference to SR-14-4, "Examiner Loan Sampling Requirements for State Member Bank and Credit Extending Nonbank Subsidiaries of Banking Organizations with $10–$50 Billion in Total Consolidated Assets." This guidance within SR-14-4 supersedes the guidance within SR-94-13, "Loan Review Requirements for On-Site Examinations" for the specified banking organizations.

2124.0.1 FULL-SCOPE INSPECTIONS AND TRANSACTION TESTING

Full-scope inspections under a risk-focused approach must be performed to fulfill the objectives of a full-scope inspection. Inspections can be adjusted, depending on the circumstances of the banking organization being evaluated. At a minimum, full-scope inspections should include sufficient procedures to reach an informed judgment on the assigned ratings for the factors addressed by the bank holding company RFI/C(D) rating system. The business of banking is fundamentally predicated on taking risks, and the components of the supervisory rating system are strongly influenced by risk exposure. Consequently, the procedures for full-scope inspections focus to a large degree on assessing the types and extent of risks to which a bank holding company and its subsidiaries are exposed, evaluating the organization's methods of managing and controlling its risk exposures, and ascertaining whether management and directors fully understand and are actively monitoring the organization's exposure to those risks. Given the Federal Reserve's responsibility for ensuring compliance with banking laws and regulations, inspections also include an appropriate level of compliance testing. (See SR-96-14.)

Historically, Federal Reserve examinations and inspections have placed significant reliance on transaction-testing procedures. For example, to evaluate the adequacy of the credit-administration process, assess the quality of loans, and ensure the adequacy of the allowance for loan and lease losses (ALLL), a high percentage of large loan amounts have traditionally been reviewed individually. Similarly, the assessment of the accuracy of regulatory reporting often has involved extensive review of reconciliations of a bank holding company's general ledger to the FR Y-9C report and other FR Y-series reports. Other similar procedures typically have been completed to ascertain compliance with applicable laws and regulations, to determine whether the banking and nonbank subsidiaries are following their internal policies and procedures and those of the bank holding company, and to evaluate the adequacy of internal control systems.

Transaction testing remains a reliable and essential inspection technique for assessing a banking organization's condition and verifying its adherence to internal policies, procedures, and controls. In a highly dynamic banking market, however, such testing is not sufficient for ensuring continued safe and sound operations. As evolving financial instruments and markets have enabled banking organizations to rapidly reposition their portfolio risk exposures, periodic assessments of a banking organization's condition, based on transaction testing alone, cannot keep pace with the moment-to-moment changes occurring in financial risk profiles.

To ensure that banking organizations have in place the processes necessary to identify, measure, monitor, and control their risk exposures, inspections must focus more on evaluating the appropriateness of a very high degree of transaction testing. Under a risk-focused approach, the degree of transaction testing should be reduced when internal risk-management processes are determined to be adequate or risks are considered minimal. However, when an organization's risk-management processes or internal controls are considered inappropriate (such as when there is an inadequate segregation of duties or when on-site testing determines that such processes or controls are lacking), additional transaction testing sufficient to fully assess the degree of risk exposure in that function or activity must be performed. In addition, if an examiner believes that a banking organization's management is being less than candid, has provided false or misleading information, or has omitted material information, then substantial on-site transaction testing should be undertaken and appropriate follow-up actions should be initiated, including the requirement of additional audit work and appropriate enforcement actions.

In most cases, full-scope inspections are conducted on or around a single date. This approach is appropriate for the vast majority of banking

organizations supervised by the Federal Reserve. However, as the largest banking organizations have undergone considerable geographic expansion and the range of their products has become more diversified, coordinating the efforts of the large number of examiners necessary to conduct inspections at a single point in time has become more difficult. To avoid causing undue burden on these banking organizations, full-scope inspections for many large companies are conducted over the course of a year, rather than over a span of weeks, in a series of targeted reviews focusing on one or two significant aspects of the bank holding company's operations. This approach to conducting full-scope inspections provides more-continuous supervisory contact with the largest bank holding companies and facilitates improved coordination of inspection efforts with other federal banking agencies. It also provides more flexibility in the allocation of examiner resources, which has been especially important as the complexity of banking markets and products has increased and led to the development of cadres of examiners with specialized skills.

2124.0.2 RISK-FOCUSED INSPECTIONS

Developments in the business of banking have increased the range of banking activities, heightening demands on examiner resources and making the need for examiners to effectively focus their activities on areas of the greatest risk even more crucial. Improved in-office planning can result in more efficient and effective on-site inspections that are focused on risks particular to specific organizations of the bank holding company. Such improved planning minimizes supervisory burden and provides for the close coordination of the supervisory efforts of the Federal Reserve with those of the other state and federal banking agencies. Improved planning also allows information requests to be better tailored to the specific organizations.

2124.0.2.1 Risk Assessment

To focus procedures on the areas of greatest risk, a risk assessment should be performed before on-site supervisory activities. The risk-assessment process highlights both the strengths and vulnerabilities of a bank holding company and provides a foundation from which to determine the procedures to be conducted during an inspection. Risk assessments identify the financial activities in which a banking organization has chosen to engage, determine the types and quantities of risks to which these activities expose the organization, and consider the quality of management and control of these risks. At the conclusion of the risk-assessment process, a preliminary supervisory strategy can be formulated for the bank holding company and its subsidiaries and for each of their major activities. Naturally, those activities that are most significant to the organization's risk profile or that have inadequate risk-management processes or rudimentary internal controls represent the highest risks and should undergo the most rigorous scrutiny and testing.

Identifying the significant activities of a bank holding company, including those activities conducted off-balance-sheet, should be the first step in the risk-assessment process. These activities may be identified through the review of prior bank examination and bank holding company inspection reports and workpapers, surveillance and monitoring reports generated by Board and Reserve Bank staffs, Uniform Bank Performance Reports and Bank Holding Company Performance Reports, regulatory reports (for example, bank Call Reports and the FR Y-9C and FFIEC 002 reports), and other relevant supervisory materials. When appropriate, the following information should be reviewed: strategic plans and budgets, internal management reports, board of directors information packages, correspondence and minutes of meetings between the bank holding company and the Reserve Bank, annual reports and quarterly SEC filings, press releases and published news stories, and stock analysts' reports. In addition, examiners should hold periodic discussions with management to gain insight into their latest strategies or plans for changes in activities or management processes.

Once significant activities have been identified, the types and quantities of risks to which these activities expose the bank holding company should be determined. This allows examiners to identify high-risk areas that should be emphasized in conducting inspections. The types of risk that may be encountered in banking activities individually or in various combinations include, but are not limited to, credit, market, liquidity, operational, legal, and reputational risks.[1] For example, lending activities are a primary source of credit and liquidity risks.

1. Appendix A defines these primary risk types.

They may also present considerable market risk (if the bank holding company or its subsidiaries are originating mortgage loans for later resale), interest-rate risk (if fixed-rate loans are being granted), or legal risk (if loans are poorly documented). Similarly, the asset-liability management function has traditionally been associated with exposures to interest-rate and liquidity risks. Operational risks are also associated with many of the transactions undertaken by this function, and market risks are associated with the investments and hedging instruments commonly used by the asset-liability management function. The quantity of risks associated with a given activity may be indicated by the volume of assets and off-balance-sheet items that the activity represents or by the portion of revenue for which the activity accounts. Activities that are new to an organization or for which exposure is not readily quantified may also represent high risks that should be evaluated during inspections.

A number of analytical techniques may be used to estimate the quantity of risk exposure, depending on the activity or risk type being evaluated. For example, to assess the quantity of credit risk in loans and commitments, the level of past-due loans, internally classified or watch list loans, nonperforming loans, and concentrations of credit exposure to particular industries or geographic regions should be considered (see section 2010.2). In addition, as part of the assessment of credit risk, the adequacy of the overall ALLL can be evaluated by considering trends in past-due, special-mention, and classified loans; historic charge-off levels; and the coverage of nonperforming loans by the ALLL. Analytical techniques for gauging the exposure of a bank holding company and its subsidiaries to interest-rate risk, as part of the evaluation of asset-liability management practices, can include a review of the historical performance of net interest margins, as well as the results of internal projections of future earnings performance or net economic value under a variety of plausible interest-rate scenarios. The measurement of the quantity of market risk arising from trading in cash and derivative instruments may take into account the historic volatility of trading revenues, the results of internal models calculating the level of capital and earnings at risk under various market scenarios, and the market value of contracts relative to their notional amounts.

Once the types and quantities of risk in each activity have been identified, a preliminary assessment of the banking organization's process to identify, measure, monitor, and control these risks should be completed. This evaluation should be based on findings from previous examination and inspection activities conducted by the Reserve Bank or other banking agencies, supplemented by the review of internal policies and procedures, management reports, and other documents that provide information on the extent and reliability of internal risk-management systems. Sound risk-management processes vary from one banking organization to another, but generally include four basic elements for each individual financial activity or function and for the organization in aggregate. These elements are (1) active board and senior management oversight; (2) adequate policies, procedures, and limits; (3) adequate risk-measurement, risk-monitoring, and management information systems; and (4) comprehensive internal audits and controls. (See sections 4070.1 (SR-95-51) and 4071.0 (SR-16-11).)

The preliminary evaluation of the risk-management process for each activity or function also helps determine the extent of transaction testing that should be planned for each area. If the organization's risk-management process appears appropriate and reliable, then a limited amount of transaction testing may well suffice. If, on the other hand, the risk-management process appears inappropriate or inadequate to the types and quantities of risk in an activity or function, examiners should plan a much higher level of transaction testing. They should also plan to conduct the most testing in those areas that comprise the most significant portions of a bank holding company's activities and, thus, typically represent high potential sources of risk.

2124.0.2.2 Preparation of a Scope Memorandum

Once the inspection planning and risk-assessment processes are completed, a scope memorandum should be prepared. A scope memorandum provides a detailed summary of the supervisory strategy for a bank holding company and assigns specific responsibilities to inspection team members. A scope memorandum should be tailored to the size and complexity of the bank holding company that is subject to review, define the objectives of each inspection, and generally include—

1. a summary of the results of the prior inspection;
2. a summary of the strategy and significant activities of the banking organization, including its new products and activities;
3. a description of the bank holding company's organization and management structure;
4. a summary of performance since the prior inspection;
5. a statement of the objectives of the current inspection;
6. an overview of the activities and risks to be addressed by the inspection; and
7. a description of the procedures that are to be performed at the inspection.

For large complex organizations operating in a number of states or internationally, the planning and risk-assessment processes are necessarily more complicated. The traditional scope memorandum may have to be broadened into a more extensive set of planning documents to reflect the unique requirements of complex bank holding companies. Examples of these planning documents include annual consolidated analyses, periodic risk assessments, and supervisory plans.

2124.0.2.3 On-Site Procedures

The amount of review and transaction testing necessary to evaluate particular functions or activities of a bank holding company generally depends on the quality of the process the company uses to identify, measure, monitor, and control the risks of an activity. When the risk-management process is considered sound, further procedures are limited to a relatively small number of tests of the integrity of the management system. Once the integrity of the management system is verified through limited testing, conclusions on the extent of risks within the function or activity are drawn based on internal management assessments of those risks rather than on the results of more-extensive transaction testing by examiners. On the other hand, if initial inquiries into the risk-management system—or efforts to verify the integrity of the system—raise material doubts as to the system's effectiveness, no significant reliance should be placed on the system. A more extensive series of tests should be undertaken to ensure that the banking organization's exposure to risk from a given function or activity can be accurately gauged and evaluated. More-extensive transaction testing is also generally completed for activities that are much more significant to a bank holding company than is completed for other areas, although the actual level of testing for these significant activities may be reduced commensurate with the quality of internal risk-management processes.

Consider, as an example, the risk exposure associated with commercial lending activities. Traditionally, examiners have reviewed a relatively high number and dollar volume of real estate–associated loans.[2] If, however, credit-administration practices are considered satisfactory, fewer loans may need be reviewed to verify that this is the case (that is, fewer loans than would be reviewed if deficiencies in credit-administration practices were suspected). This review may be achieved through a valid statistical sampling technique, when appropriate. It should be noted that if credit-administration practices are initially considered sound, but if loans reviewed to verify this raise doubts about the accuracy of internal assessments or the compliance with internal policies and procedures, the number and volume of loans subject to review should generally be expanded. Examiners should thus review a sufficient number of loans in order to ensure that the level of risk is clearly understood, an accurate determination of the adequacy of the ALLL can be made, and the deficiencies in the credit risk-management process can be comprehensively detailed.

2124.0.2.4 Evaluation of Audit Function as Part of Assessment of Internal Control Structure

A bank holding company's internal control structure is critical to its safe and sound functioning in general and to its risk-management system in particular. When properly structured, internal controls promote effective operations and reliable financial and regulatory reporting; safeguard assets; and help to ensure compliance with laws, regulations, and internal policies and procedures. In many banking organizations, internal controls are tested by an independent

2. Guidance on the selection of loans for review is provided in SR-94-13, "Loan Review Requirements for On-Site Examinations." The guidance within SR-94-13 is superseded by SR-14-4, "Examiner Loan Sampling Requirements for State Member Bank and Credit Extending Nonbank Subsidiaries of Banking Organizations with $10–$50 Billion in Total Consolidated Assets," but only for these banking organizations. SR-14-4 clarifies expectations for the assessment of material retail credit portfolios for these institutions (see appendix 1 at section 2010.2.11).

internal auditor who reports directly to the board of directors or its audit committee. However, in some smaller banking organizations whose size and complexity of operations do not warrant an internal audit department, reviews of internal controls may be conducted by other personnel independent of the area subject to review.

Because the audit function is an integral part of a bank holding company's assessment of its internal control system, examiners must include a review of the organization's control-assessment activities in every inspection. Such reviews help identify significant risks and facilitate a comprehensive evaluation of the organization's internal control structure and also provide information to determine the inspection procedures that should be completed in assessing internal controls for particular functions and activities and for the bank holding company overall. When conducting this review, examiners should evaluate the independence and competence of the personnel conducting control assessments and the effectiveness of the assessment program in covering the bank holding company's significant activities and risks. In addition, examiners should meet with the internal auditors or other personnel responsible for evaluating internal controls. Examiners should review internal control risk assessments, work plans, reports, workpapers, and related communications with the audit committee or board of directors.

Depending on the size and complexity of the activities conducted by a bank holding company, the examiner should also consider conducting a similar review of the work performed by the company's external auditors. Such a review often provides added insight into key risk areas by detailing the nature and extent of the external auditors' testing of those areas.

2124.0.2.5 Evaluation of Overall Risk-Management Process

To highlight the importance of a banking organization's risk-management process, bank holding companies are assigned a risk-management rating on a five-point scale as a significant part of the evaluation of the management components of the bank holding company RFI/C(D) rating system. (See section 4070.0.) In addition, U.S. branches and agencies of foreign banking organizations are assigned a similar rating under the ROCA rating system.[3] These risk-management ratings encompass evaluations of the quality of risk-management processes for all significant activities and all types of risks. As such, they should largely summarize conclusions on the adequacy of risk-management processes for each individual function or activity evaluated.

In assigning risk-management ratings, it is important that examiners consider the quality of the risk-management process for the bank holding company overall, as well as for each individual function. At smaller bank holding companies engaged in traditional banking and nonbanking activities, relatively basic risk-management processes established for each significant activity, such as lending or asset-liability management, may be adequate to allow senior management to effectively manage the organization's overall risk profile. On the other hand, at larger bank holding companies that are typically engaged in more-complex and widely diversified activities, effective risk-management systems must evaluate various functional management processes in combination so that aggregate risk exposures can be identified and monitored by senior management. Management information reports should typically be generated for the overall organization, as well as for individual functional areas. Some aggregate or specific company-wide limits may also be needed for the principal types of risks that are relevant to the company's activities.

A critical aspect of ensuring that a bank holding company's risk-management and control procedures remain adequate is the ongoing testing of the strength and integrity of these procedures and the extent to which the procedures are understood and followed throughout the organization. When assigning a risk-management rating, examiners should assess the adequacy of the company's efforts to ensure that its procedures are being followed. The company's validation efforts must be conducted by individuals who have proper levels of organizational independence and expertise, such as internal or external auditors, internal risk-management units, or managers or other professionals of the bank holding company who have no direct connection to the activities for which procedures are being assessed.

3. U.S. branches and agencies of foreign banking organizations are assigned separate ROCA ratings for risk management, operational controls, compliance, and asset quality, under guidance included in SR-00-14, "Enhancements to the Interagency Program for Supervising the U.S. Operations of Foreign Banking Organizations."

2124.0.2.6 Evaluation of Compliance with Laws and Regulations

Compliance with relevant laws and regulations should be assessed at every inspection. The steps taken to complete these assessments, however, will vary depending on the circumstances of the bank holding company being reviewed. When an organization has a history of satisfactory compliance with relevant laws and regulations or an effective compliance function, only a relatively limited degree of transaction testing need be conducted to assess compliance. For example, when evaluating compliance with the appraisal requirements of Regulation Y at a bank holding company with a formal compliance function, compliance may be ascertained by reviewing the scope and findings of internal and external audit activities, evaluating the internal appraisal-ordering and -review processes, and sampling a selection of appraisals for compliance, as part of the supervisory loan-review process. On the other hand, at bank holding companies that have a less satisfactory compliance record or that lack a compliance function, more appraisals would naturally need to be tested to assess the overall compliance with the appraisal requirements of Regulation Y.

2124.0.2.7 Documentation of Supervisory Findings

The examiners' workpaper documentation of supervisory findings is necessary for Reserve Bank management to objectively verify the inspection work performed. Such documentation also provides a source of information on the condition and prospects of a bank holding company that is invaluable for planning future reviews. Most important, examiners' workpaper documentation provides support for the conclusions and recommendations detailed in the inspection report.

2124.0.2.8 Communication of Supervisory Findings

Effective and open communication between bank supervisory agencies and the board of directors and management of bank holding companies is essential to ensuring that the results of inspections are fully understood; the directorship and management are aware of any identified deficiencies; and, when necessary, they take appropriate corrective actions.

2124.0.3 INSPECTION OBJECTIVES

1. To ensure that the bank holding company has in place the processes necessary to identify, measure, monitor, and control its risk exposures for each of its activities or functions.
2. To improve inspection efficiencies by stressing increased in-office planning of inspections, using a risk-focused emphasis.
3. To identify and assess significant on- and off-balance-sheet activities and the greatest types and quantities of risk exposures and vulnerabilities to the bank holding company, tailoring the extent of transaction testing to the results of this review and other inspections' findings.
4. To review and assess the effectiveness and adequacy of documentation of the bank holding company's control and assessment activities and arrangements, including its internal control structure, and the qualifications of internal and external auditors and other independent personnel involved in the program.
5. To emphasize the preparation of a risk-focused scope memorandum that is tailored to the size and complexity of the bank holding company under inspection.
6. To evaluate compliance with laws and regulations.
7. To adequately document and communicate inspection supervisory findings, recommendations, and conclusions.

2124.0.4 INSPECTION PROCEDURES

1. Identify the significant on- and off-balance-sheet activities of the bank holding company.
   a. Review prior inspection reports and workpapers, surveillance and monitoring reports generated by the Board and Reserve Bank staff, Uniform Bank Performance Reports and Bank Holding Company Performance Reports, regulatory reports (for example, bank Call Reports and FR Y-series and other FFIEC reports), and other relevant supervisory materials.
   b. Review strategic plans and budgets; internal management reports; board of directors information packages; correspondence and minutes, including minutes of meetings held between the bank holding company and the Reserve Bank; annual reports and quarterly SEC filings; press releases and published news stories; and stock analysts' reports.

2. Hold periodic discussions with management to gain insight into recently adopted strategies or plans to change activities or management processes.
3. Once the significant activities have been identified, determine and analyze the types (for example, credit, market, liquidity, operational, legal, and reputational) and quantities of risks to which those activities expose the bank holding company, placing greater inspection emphasis on the high-risk areas.
4. Develop an assessment of the processes that are used to identify, measure, monitor, and control the risks. Focus on the extent of board and senior management oversight; the adequacy of policies, procedures, limits, risk-measurement, risk-monitoring, and management information systems; and the existence of adequately documented internal audits and controls.
5. Prepare a scope memorandum tailored to the size and complexity of the bank holding company under inspection.
6. Conduct limited tests of the integrity of the risk-management system. Conduct more-extensive transaction testing for those areas of a bank holding company that are very significant compared with other areas, adjusting the level of transaction testing to the quality of internal risk-management processes. If initial inquiries or efforts to verify the system raise material doubts as to its effectiveness, place no reliance on the integrity of the bank holding company's risk-management system and conduct more-extensive transaction testing.
7. Review the bank holding company's risk-assessment control activities, including an assessment of internal controls for particular functions and activities and for the bank holding company overall.
   a. Evaluate the independence and competence of the personnel conducting control assessments and the effectiveness of the assessment program in covering the bank holding company's significant activities and risks.
   b. Meet the independent external and internal auditors and other personnel responsible for evaluating internal controls and review the internal control risk assessments, work plans, reports, workpapers, and related communications with the audit committee or the board of directors.
8. Assess the adequacy of efforts to ensure that the current risk-management and control procedures are being followed.
9. Assess compliance with laws and regulations, adjusting the extent of transaction testing with the organization's history of satisfactory compliance.
10. Document all work performed and the supervisory findings. Include information on the condition and prospects of the bank holding company and its significant subsidiaries, as well as the inspection's conclusions and recommendations.

2124.0.5 APPENDIX A—DEFINITIONS OF RISK TYPES EVALUATED AT INSPECTIONS

1. *Credit risk* arises from the potential that a borrower or counterparty will fail to perform on an obligation.
2. *Market risk* is the risk to a bank holding company's condition resulting from adverse movements in market rates or prices, such as interest rates, foreign-exchange rates, or equity prices.
3. *Liquidity risk* is the potential that a bank holding company will be unable to meet its obligations as they come due because of an inability to liquidate assets or obtain adequate funding (referred to as "funding liquidity risk") or that it cannot easily unwind or offset specific exposures without significantly lowering market prices because of inadequate market depth or market disruptions ("market liquidity risk").
4. *Operational risk* arises from the potential that inadequate information systems, operational problems, breaches in internal controls, fraud, or unforeseen catastrophes will result in unexpected losses.
5. *Legal risk* arises from the potential that unenforceable contracts, lawsuits, or adverse judgments can disrupt or otherwise negatively affect the operations or condition of a bank holding company.
6. *Reputational risk* is the potential that negative publicity on a bank holding company's business practices, whether true or not, will cause a decline in the customer base, costly litigation, or revenue reductions.

What's New In This Revised Section

Effective July 2014, this section was revised to include Appendix B — Managing Foreign Exchange Settlement Risks for Physically Settled Transactions. See SR-13-24. This guidance sets forth seven principles or "guidelines" for managing foreign exchange transaction settlement risks. The Federal Reserve supports these principles as part of its continuing effort to promote the global financial system's ability to withstand severe market disruptions. Institutions covered by SR-13-24 should apply the seven guidelines to their foreign exchange activities with the stated clarifications regarding application of the guidance in the United States.

The Federal Reserve adopted a new framework for the consolidated supervision of large financial institutions on December 17, 2012.[1] The framework strengthens traditional microprudential supervision and regulation to enhance the safety and soundness of individual firms. It also incorporates macroprudential considerations to reduce potential threats to the stability of the financial system and to provide insights into financial market trends. The consolidated supervision framework has two primary objectives:

- *Enhancing resiliency of a firm to lower the probability of its failure or inability to serve as a financial intermediary.*
  Each firm is expected to ensure that the consolidated organization (or the combined U.S. operations in the case of foreign banking organizations) and its core business lines[2] can survive under a broad range of internal or external stresses. This requires financial resilience by maintaining sufficient capital and liquidity, and operational resilience by maintaining effective corporate governance, risk management, and recovery planning.
- *Reducing the impact on the financial system and the broader economy in the event of a firm's failure or material weakness.*
  Each firm is expected to ensure the sustainability of its critical operations[3] and banking offices[4] under a broad range of internal or external stresses. This requires, among other things, effective resolution planning that addresses the complexity and the interconnectivity of the firm's operations.

These objectives are consistent with key provisions of the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). These provisions include enhanced prudential standards, which provide the Federal Reserve with the flexibility to tailor the application of these standards to individual firms or groups of firms.[5] (See SR-12-17/CA-12-14 and the supplemental guidance in SR-13-23.)

2124.05.1 FRAMEWORK APPLICABILITY

The new framework is designed to support a tailored supervisory approach that accounts for the unique risk characteristics of each firm, including the nature and degree of potential systemic risks inherent in a firm's activities and operations, as well as broader trends across firms. This framework applies to the following institutions:

- *Large Institution Supervision Coordinating Committee (LISCC) firms:* the largest, most complex U.S. and foreign financial organizations subject to consolidated supervision by the Federal Reserve. Nonbank financial companies designated by the Financial Stability Oversight Council (FSOC) for supervision by the Federal Reserve are included in the LISCC portfolio. LISCC firms are considered to pose the greatest systemic risk to the U.S. economy.
  The LISCC is a multidisciplinary body that

1. The previous framework, SR-99-15, "Risk-Focused Supervision of Large Complex Banking Organizations," is superseded. In addition, for the firms described in subsection 2124.05.1, "Framework Applicability," the framework for consolidated supervision set forth in SR-08-9/CA-08-12, "Consolidated Supervision of Bank Holding Companies and the Combined U.S. Operations of Foreign Banking Organizations," is no longer applicable.

2. "Core business lines" are those business lines (including associated operations, services, functions, and support) that, in the firm's view, upon failure would result in a material loss of revenue, profit, or franchise value.

3. "Critical operations" are those operations (including associated services, functions, and support) that if they were to fail or be discontinued could pose a threat to the financial stability of the United States.

4. "Banking offices" are defined as U.S. depository institution subsidiaries, as well as the U.S. branches and agencies of foreign banking organizations.

5. 12 U.S.C. 5365 and 12 U.S.C. 5365(a)(2).

oversees supervision and evaluates conditions of supervised firms. The committee also develops cross-firm perspectives and monitors interconnectedness and common practices that could lead to greater systemic risk.
- *Large Banking Organizations (LBOs):* domestic bank and savings and loan holding companies with consolidated assets of $50 billion or more that are not included in the LISCC portfolio.
- *Large Foreign Banking Organizations (Large FBOs):* foreign banking organizations with combined assets of U.S. operations of $50 billion or more that are not included in the LISCC portfolio.

In certain instances, the framework applies to the intermediate holding company that is the primary focus of regulations and supervisory activities for the consolidated entity.

2124.05.2 FRAMEWORK OVERVIEW

The supervisory framework comprises the framework's sections' A, B, and C. Sections A and B specifies the Federal Reserve's expectations across the following core areas of supervisory focus:

A. Enhancing Resiliency of a Firm
   (1) Capital and Liquidity Planning and Positions
   (2) Corporate Governance
   (3) Recovery Planning
   (4) Management of Core Business Lines
B. Reducing the Impact of a Firm's Failure
   (1) Management of Critical Operations
   (2) Support for Banking Offices
   (3) Resolution Planning
   (4) Additional Macroprudential Supervisory Approaches to Address Risks to Financial Stability
C. Conduct of Supervisory Activities

The Federal Reserve may periodically identify additional supervisory priorities beyond these core areas of focus as necessary to enhance firm-specific supervision and develop cross-firm perspectives.

Subsection 2124.05.5, ''Conduct of Supervisory Activities,'' (framework section C) outlines the conduct of supervisory activities used to maintain a comprehensive understanding and assessment of each firm. Effective consolidated supervision requires strong, cooperative relationships between the Federal Reserve and other bank supervisors and functional regulators. The Federal Reserve generally relies to the fullest extent possible on the information and assessments provided by other supervisors and regulators to support effective supervision. Supervisory agencies engaged in the supervision of large financial institutions continue to enhance formal and informal discussions to jointly identify and address key vulnerabilities, and to coordinate supervisory strategies for these firms.

As a general matter, this framework is applicable in circumstances when the consolidated organization and its banking offices are in at least satisfactory condition and there are no material weaknesses or risks across these core areas of supervisory focus. The Federal Reserve applies additional supervisory expectations, and undertakes related activities, to address identified concerns including areas subject to formal or informal enforcement action.

2124.05.3 ENHANCING RESILIENCY OF A FIRM

2124.05.3.1 Capital and Liquidity Planning and Positions

The financial crisis demonstrated the need for stronger regulatory and supervisory assessments of firms' financial resiliency.[6] The Federal Reserve noted significant weaknesses in the adequacy of firms' point-in-time regulatory capital to cover accumulated and prospective risks, as well as in firms' liquidity buffers and risk-management practices.[7] These weaknesses contributed to the failure or near failure of many financial firms and exacerbated the crisis. To support effective capital and liquidity planning, and the adequacy of capital and liquidity positions, each firm should:

a) Maintain strong capital and liquidity positions that not only comply with regulatory requirements, but also support the firm's ongoing ability to meet its obligations to creditors and other counterparties, as well as

6. See the Board's final rule on capital plan requirements for large bank holding companies (76 Fed. Reg. 74631, December 1, 2011); SR-10-6, ''Interagency Policy Statement on Funding and Liquidity Risk Management'' (75 *Fed. Reg.* 13656, March 22, 2010); and section 4066.0 of this manual.

7. The capital components of this framework, including those related to stress testing, will apply to savings and loan holding companies after they become subject to minimum regulatory capital requirements.

continue to serve as a financial intermediary through periods of stress.
b) Have in place robust internal processes that enable the firm to maintain capital and liquidity commensurate with its unique risks under normal and stressful conditions, and to provide timely restoration of financial buffers in the event of drawdown.
c) Maintain processes that enable the identification and measurement of potential risks to asset quality, earnings, cash flows, and other primary determinants of capital and liquidity positions.
d) Utilize comprehensive projections of the level and composition of capital and liquidity resources, supported by rigorous and regular stress testing to assess the potential impact of a broad range of expected and potentially adverse scenarios.
e) Maintain sound risk measurement and modeling capabilities, supported by comprehensive data collection and analysis, independent validation, and effective governance, policies, and controls.[8]
f) Establish goals for capital and liquidity positions that are approved by the firm's board of directors and reflect the potential impact of legal or regulatory restrictions on the transfer of capital or liquidity between legal entities.
g) Maintain independent internal audit and other review functions with appropriate staff expertise, experience, and stature in the organization to monitor the adequacy of capital and liquidity risk measurement and management processes.

2124.05.3.2 Corporate Governance

In order for a firm to be sustainable under a broad range of economic, operational, legal or other stresses, its board of directors (or equivalent for the U.S. operations of FBOs) should provide effective corporate governance with the support of senior management. The board is expected to establish and maintain the firm's culture, incentives, structure, and processes that promote its compliance with laws, regulations, and supervisory guidance. Each firm's board of directors and committees, with support from senior management, should:

a) Maintain a clearly articulated corporate strategy and institutional risk appetite. The board should set direction and oversight for revenue and profit generation, risk management and control functions, and other areas essential to sustaining the consolidated organization.
b) Ensure that the firm's senior management has the expertise and level of involvement required to manage the firm's core business lines, critical operations, banking offices, and other material entities.[9] These areas should receive sufficient operational support to remain in a safe and sound condition under a broad range of stressed conditions.
c) Maintain a corporate culture that emphasizes the importance of compliance with laws and regulations and consumer protection, as well as the avoidance of conflicts of interest and the management of reputational and legal risks.
d) Ensure the organization's internal audit, corporate compliance, and risk management and internal control functions are effective and independent, with demonstrated influence over business-line decision making that is not marginalized by a focus on short-term revenue generation over longer-term sustainability.[10]
e) Assign senior managers with the responsibility for ensuring that investments across business lines and operations align with corporate strategies, and that compensation arrangements and other incentives are consistent with the corporate culture and institutional risk appetite.[11]
f) Ensure that management information systems (MIS) support the responsibilities of the board of directors to oversee the firm's core business lines, critical operations, and other core areas of supervisory focus.

2124.05.3.3 Recovery Planning

Robust recovery planning is central to ensuring the ongoing resiliency of a firm's consolidated operations as well as its core business lines, critical operations, banking offices, and other material entities. Each firm should plan for potential financial or operational weaknesses

8. See SR-11-7, and section 2126.0 of this manual.

9. "Material entities" are subsidiaries or foreign offices of the firm that are significant to the activities of a core business line or critical operation.

10. See SR-08-8/CA-08-11, and section 2124.07 of this manual.

11. Refer to "Guidance on Sound Incentive Compensation Policies" (75 Fed. Reg. 36395, June 25, 2010) and section 2068.0 of this manual.

and identify actions to correct those weaknesses. Therefore, each firm should:

a) Maintain clearly documented quantitative and qualitative criteria that would trigger timely implementation of specific elements of the firm's recovery plan and provide for more rigorous remediation activities if initial actions prove insufficient.
b) Ensure that trigger events reflect a sufficiently broad range of market- and firm-specific stresses across financial, operational, reputational, legal, and compliance risks.
c) Ensure that recovery planning reflects a holistic view of sustainability and resiliency. Recovery planning should be closely integrated with resolution planning, capital and liquidity planning, and other aspects of financial contingency, crisis management, and business continuity planning.[12]
d) Undertake recovery testing and training exercises that consider a broad range of internal and external risk scenarios and account for interconnectivities across operations and legal entities.
e) Ensure that the recovery plan is updated as needed, and reflects lessons learned from reviews of trigger events, testing, and training exercises.
f) Ensure that recovery planning is sufficiently integrated into corporate governance structures and processes, subject to independent validation, and effectively supported by related MIS reporting to the board and its committees.

2124.05.3.4 Management of Core Business Lines

Effective management of core business lines is essential to ensuring the resilience of the consolidated organization, as these activities are the primary drivers of the firm's revenue generation, profitability, and franchise value. For this reason, a firm's corporate governance should extend (as discussed in subsection 2124.05.3.2, "Corporate Governance" (*framework section A.2*)) to the management of each core business line. Each core business line should have:

- Business-line senior management with qualifications and experience commensurate with the size and complexity of related activities and operations;
- A strategic planning process that ensures areas of growth and innovation are effectively managed;
- Appropriate compensation and other incentives that are consistent with the institutional risk appetite and in compliance with laws and regulations;
- An independent and strong risk-management framework that supports identification, measurement, assessment, and control of the full spectrum of risks; and
- Timely identification and resolution of audit, compliance, and regulatory issues

2124.05.4 REDUCING THE IMPACT OF A FIRM'S FAILURE

2124.05.4.1 Management of Critical Operations

The failure or discontinuance of any of a firm's critical operations could weaken the U.S. economy or pose a threat to the financial stability of the United States. Each of the supervisory expectations outlined around management of core business lines (see subsection 2124.05.3.4, "Management of Core Business Lines" (*framework section A.4*)) applies equally to management of critical operations to ensure their financial and operational resilience. Additionally, each firm should ensure that critical operations are sufficiently resilient to be maintained, continued, and funded even in the event of failure or material financial or operational distress. These expectations should be fully reflected in recovery and resolution planning.

2124.05.4.2 Support for Banking Offices

The Federal Reserve's consolidated supervision program has historically focused on protecting the safety and soundness of U.S. depository institution subsidiaries of bank holding companies and the U.S. branches and agencies of foreign banking organizations (collectively defined as banking offices). This is due to the risks posed by banking offices' access to the federal safety net. Specifically, these offices pose risks to the payment system, the Federal Reserve's discount window, and—in the case of most U.S. depository institutions—federal deposit insurance funds.

12. Business continuity expectations include adherence with expectations set forth in SR-03-9, including the geographic diversity and resiliency of data centers and operations, and testing of recovery and resumption arrangements.

A consolidated organization should serve as a source of financial and managerial strength to its banking offices. The activities of the parent company and affiliated nondepository subsidiaries should not present material risks to affiliated banking offices, the consolidated organization itself, or to the consolidated organization's ability to support its banking offices.[13] Each firm should:

a) Provide for the strength and resiliency of its banking offices, ensuring prompt financial and operational support so that each office remains in a safe and sound condition under a broad range of stressed conditions.
b) Ensure that the activities of the parent company and nondepository institution subsidiaries do not present undue direct or indirect risks to the safety and soundness of banking offices. This includes the transmission of financial, operational, legal, compliance, or reputational risks that may undermine public confidence in the financial strength of its banking offices.
c) Maintain sufficient liquidity, cash flow, and capital strength at the parent company and nondepository institution subsidiaries to service debt obligations and cover fixed charges. The parent company needs to consider whether there are any legal or regulatory restrictions on financial transfers between legal entities within the organization.
d) Implement and maintain effective policies, procedures, and systems to ensure compliance with applicable laws and regulations. This includes compliance with respect to covered transactions subject to the Board's Regulation W, which implements sections 23A and 23B of the Federal Reserve Act and limits a bank's transactions with its affiliates.[14]

13. Due to structural differences, there are important distinctions in the forms of support provided to U.S. depository institution subsidiaries versus those provided to the U.S. branches and agencies of foreign banks. For example, branches/agencies do not hold capital and have differing business and liquidity profiles, governance mechanisms, and regulatory requirements than depository institutions. Therefore, the Federal Reserve will consider these differences in its implementation of this supervisory framework for the U.S. branches and agencies of FBOs, and expects parent FBOs and their U.S. branches and agencies to do the same. The extent of supervisory activity undertaken to assess the adequacy of parent company support for U.S branches and agencies of FBOs is scaled to the condition, size, and interconnectedness of these offices.

14. See SR-03-2, and section 2020.1 of this manual.

2124.05.4.3 Resolution Planning

To promote financial stability, the Dodd-Frank Act requires each bank holding company with consolidated assets of $50 billion or more, as well as nonbank financial companies designated by the FSOC, to develop and maintain plans for rapid and orderly resolution in the event of material financial distress or failure. These plans should be utilized as an element of the firm's strategic planning and address the complexity and interconnectivity of the firm's operations.[15]

The Federal Reserve and the FDIC jointly review a firm's resolution plan relative to supervisory requirements, including:

a) The firm's strategic analysis describing its plans for rapid and orderly resolution under the U.S. Bankruptcy Code (or other relevant insolvency regimes). This strategy must not pose systemic risk and must exclude reliance on extraordinary support from the United States or any other government to prevent failure of the firm.
b) The firm's strategy for maintaining and funding material entities, critical operations, and core business lines in the event of material financial distress.
c) Analysis of potential impediments to resolution, and actions to make the firm more resolvable or otherwise reduce its complexity and interconnectivity.
d) Analysis of whether the failure of a major counterparty would likely result in the material financial distress or failure of the firm.
e) The manner and extent to which an insured depository subsidiary is adequately protected from risks arising from the activities of nondepository subsidiaries.
f) For a U.S. firm with foreign operations, its strategy for addressing the risks arising from these foreign operations to its U.S. operations, and its ability to maintain core business lines and critical operations in foreign jurisdictions.
g) Analysis of whether resolution planning is sufficiently integrated into corporate governance structures and processes, subject to independent validation, and effectively supported by related MIS reporting to the board of directors and its committees.

15. Refer to 12 C.F.R. 243 (Federal Reserve) and 12 C.F.R. 381 (FDIC) for the ''Resolution Plans Required'' regulations. See also, 76 *Fed. Reg.* 67323, November 1, 2011.

2125.05.4.4 Additional Macroprudential Supervisory Approaches to Address Risks to Financial Stability

The financial crisis demonstrated that too narrow a focus on the safety and soundness of individual firms can result in a failure to detect and address emerging threats to financial stability that arise across many firms. The Dodd-Frank Act requires the Federal Reserve to consider the broader risks to financial stability posed by individual companies and through the interconnectedness among these companies. See section 1040.0.3 of this manual.

The Federal Reserve aims to reduce systemic risks by increasing the capacity of firms and markets to absorb shocks when problems occur, and by reducing potential costs in the event of financial distress or failure of a systemically important institution. Supervision carried out under this framework will support a variety of macroprudential supervisory approaches beyond those already discussed, including:

a) Using insights developed through microprudential supervision and related data collection and analysis to identify, understand, and assess potential systemic risks. Areas of review could include, for example, emerging trends in critical operations, interconnectedness, rapidly expanding markets, cyclical industries, and financial products lacking substitutes or effecting large market segments.
b) Identifying potential risks to financial stability indicated by the information in supervisory stress tests and through trends in scenarios employed by firms in their internal stress tests.
c) Using comparative and aggregate analysis to monitor industry practices, common investment or funding strategies, changes in degree or form of financial interconnectedness, or other developments with implications for financial stability.
d) Coordinating with the Federal Reserve's supervision of systemically important financial market utilities to identify and address risks related to payment, clearing, and settlement activities, as well as to identify potential structural vulnerabilities.
e) Working closely with the FSOC and other regulators and supervisors to support the designation and supervision of systemically important nonbank firms, and to enhance the monitoring of systemic risk.
f) Enhancing international coordination with foreign counterparts, including national supervisors and international bodies such as the Basel Committee on Bank Supervision, the Financial Stability Board, and the Senior Supervisors Group. These activities focus on enhancing oversight of internationally active financial firms and markets and on minimizing the opportunities for firms to take advantage of weaker or inconsistent regulations.

2124.05.5 CONDUCT OF SUPERVISORY ACTIVITIES

The Federal Reserve uses a range of supervisory activities to maintain a comprehensive understanding and assessment of each firm, including:

a) Coordinated horizontal reviews involve examination of several institutions simultaneously, encompassing firm-specific supervision and the development of cross-firm perspectives. The Federal Reserve recognizes the priority of these reviews through the dedication of multidisciplinary skills and experienced staff. Examples include analysis of capital adequacy and planning via the Comprehensive Capital Analysis and Review (CCAR), as well as horizontal evaluations of resolution plans and incentive compensation practices.
b) Firm-specific examination and continuous monitoring activities[16] are undertaken to maintain an understanding and assessment across the core areas of supervisory focus for each firm. These activities include review and assessment of changes in strategy, inherent risks, control processes, and key personnel, and follow-up on previously identified concerns (for example, areas subject to enforcement actions or other supervisory issues, or emerging vulnerabilities).
c) In developing and executing a detailed supervisory plan for each firm, the Federal Reserve generally relies to the fullest extent possible on the information and assessments provided by other relevant supervisors and functional regulators. The Federal Reserve

16. "Continuous monitoring activities" include meetings with a banking organization's management; analysis of internal MIS reports, market indicators, and other internal and external information; review of internal and external audit findings; and coordination with other relevant supervisors and functional regulators and utilization of their work as appropriate.

actively participates in interagency information sharing and coordination, consistent with applicable laws, to promote comprehensive and effective supervision and limit unnecessary duplication of information requests. Supervisory agencies continue to enhance formal and informal discussions to jointly identify and address key vulnerabilities, and to coordinate supervisory strategies for large financial institutions.

d) In certain instances, supervisors may be able to rely on a firm's internal audit or internal control functions in developing a comprehensive understanding and assessment.

2124.05.6 APPENDIX A

2124.05.6.1 Risk Transfer Considerations When Assessing Capital Adequacy

The following discussion, SR-13-23, provides supplemental guidance to SR-12-17/CA letter 12-14 pertaining to its supervisory focus on an institution's capital adequacy and liquidity sufficiency. The supplemental guidance centers on how certain risk transfer transactions affect assessments of capital adequacy at large financial institutions (hereafter referred to as firms).[17] It provides clarification on supervisory expectations when assessing a firm's capital adequacy in certain circumstances when the risk-based capital framework may not fully capture the residual risks of a transaction.[18]

Risk mitigation techniques can reduce a firm's level of risk. In general, the Federal Reserve views a firm's engagement in risk-reducing transactions as a sound risk-management practice. There are, however, certain risk-reducing transactions for which the risk-based capital framework may not fully capture the residual risks that a firm faces on a post-transaction basis. As a result of inquiries and discussions with market participants, the Federal Reserve has identified specific characteristics of risk transfer transactions that give rise to this concern and on which further guidance is needed, including cases in which

- A firm transfers the risk of a portfolio to a counterparty (which may be a thinly capitalized special purpose vehicle (SPV)) that is unable to absorb losses equal to the risk-based capital requirement for the risk transferred; or
- A firm transfers the risk of a portfolio to an unconsolidated, "sponsored" affiliate entity of the firm (which also may be an SPV).

In cases involving unaffiliated counterparties, while the transactions may result in a significant reduction in a firm's risk-weighted assets and associated capital requirements under the regulatory capital framework, the firm may nonetheless face residual risks. These residual risks arise because the effectiveness of a firm's hedge involving a thinly capitalized SPV counterparty would be limited to the loss absorption capacity of the SPV itself. In cases involving unconsolidated "sponsored" affiliates of the firm, the residual risk arises from the implicit obligation the sponsoring firm may have to provide support to the affiliate in times of stress. SR-13-23 addresses how the Federal Reserve supervisory staff will view such risk-reducing transactions[19] in evaluating a firm under the Board's capital plan rule and the associated annual Comprehensive Capital Analysis and Review (CCAR).[20]

In the case of a risk transfer transaction with a non-affiliated, limited-recourse SPV or other counterparty with limited loss-absorption capacity, Federal Reserve supervisory staff will evaluate the difference between the amount of capital required for the hedged exposures before the risk transfer transaction and the counterparty's loss-absorbing resources. When evaluating capital adequacy, including in the context of CCAR, supervisory staff will evaluate whether a firm holds sufficient capital in addition to its minimum regulatory capital requirements to cover this difference.[21] In addition, when a firm engages in such a risk transfer transaction, the

17. This guidance applies to large financial institutions that are domestic bank and savings and loan holding companies with consolidated assets of $50 billion or more and foreign banking organizations with combined assets of U.S. operations of $50 billion or more.

18. See 12 CFR 217. The risk-based capital framework establishes risk-based and leverage capital requirements for banking organizations, including top-tier savings and loan holding companies, except those that are substantially engaged in insurance underwriting or commercial activities. This guidance would apply to such entities at such time as risk-based and leverage capital requirements become applicable to them.

19. While the cases described are examples, the principles set forth should apply to other transactions that call into question the degree to which risk transfer has occurred.

20. See 12 CFR 225.8(d)(2)(i). For additional guidance on CCAR, refer to the Federal Reserve's website at www.federalreserve.gov/bankinforeg/ccar.htm. The capital plan rule and CCAR apply only to bank holding companies with total consolidated assets of $50 billion or more.

21. Supervisory staff may also analyze whether the counterparty has liabilities in addition to the specific risk transfer transaction.

firm should be able to demonstrate that it reflects the residual risk in its internal assessment of capital adequacy and maintains sufficient capital to address such risk. In this regard, a commitment by a third party to provide additional capital in a period of financial stress would not be counted toward the loss-absorbing capacity of the counterparty.

Example: A firm has a $100 portfolio that has a capital requirement of $8. If the firm undertakes a transaction to transfer the risk of this portfolio to an unaffiliated SPV with paid-in capital of $3, then the firm would need to be able to demonstrate that, in addition to meeting its minimum regulatory capital requirements, the firm has sufficient capital to cover the $5 difference between the SPV's capital and the capital requirement associated with the portfolio.

In the case of risk transfer to an unconsolidated, ''sponsored'' affiliated entity, the nature of the firm's relationship with the entity calls into question the degree of risk transfer in the transaction. Firms are discouraged from entering into such transactions, which generally do not involve effective risk transfer because of the sponsored entity's ongoing relationship with the firm and, as noted above, the implicit obligation that the firm may have to provide capital to the sponsored entity in a period of financial stress affecting the sponsored entity. Firms engaging in such transactions should presume for the purpose of their internal capital adequacy assessment as well as for capital planning purposes that no risk transfer has occurred.

Supervisors will strongly scrutinize risk transfer transactions that result in substantial reductions in risk-weighted assets, including in supervisors' assessment of a firm's overall capital adequacy, capital planning, and risk management through CCAR. Based on an assessment of the risks retained by the firm, the Board may in particular cases determine not to recognize a transaction as a risk mitigant for risk-based capital purposes.[22] Firms should bring these types of risk transfer transactions to the attention of their senior management and supervisors. Supervisors will evaluate whether a firm can adequately demonstrate that the firm has taken into account any residual risks in connection with the transaction.

2124.05.7 APPENDIX B—MANAGING FOREIGN EXCHANGE SETTLEMENT RISKS FOR PHYSICALLY SETTLED TRANSACTIONS

The Federal Reserve notes that the Basel Committee on Banking Supervision (Committee), with input from the Federal Reserve,[23] published ''Supervisory Guidance for Managing Risks Associated with the Settlement of Foreign Exchange Transactions'' (guidance) in February 2013. This guidance sets forth seven principles or ''guidelines'' for managing foreign exchange transaction-settlement risks. The Federal Reserve considers this guidance on foreign exchange settlement risks to be a component of its current, broad-based focus on banking institutions' foreign exchange activities.

The Federal Reserve supports these principles as part of its continuing effort to promote the global financial system's ability to withstand severe market disruptions, and has determined that the institutions subject to SR-13-24 (covered institutions)[24] should apply the seven guidelines, which are summarized below (see sections 3.1 through 3.7 of the guidance), to their foreign exchange activities, with the following clarifications regarding application of the guidance in the United States.[25]

22. See generally 12 CFR 217.1(d)(1), (d)(3), and (d)(5). In addition, under the Board's current capital adequacy guidelines for bank holding companies and state member banks (banking organizations), the Board may determine that the regulatory capital treatment for a banking organization's exposure or other relationship to an entity not consolidated on the banking organization's balance sheet is not commensurate with the actual risk relationship of the banking organization to the entity. In making this determination, the Board may require the banking organization to treat the entity as if it were consolidated onto the balance sheet of the banking organization for risk-based capital purposes and calculate the appropriate risk-based capital ratios accordingly, all as specified by the Board. See 12 CFR parts 208 and 225, Appendix A, section I.

23. This guidance applies to large financial institutions supervised by the Federal Reserve, as defined in SR-12-17/CA-12-14. This guidance does not apply to community and regional banking organizations, defined as those with less than $50 billion in total consolidated assets, unless the banking organization engages in significant foreign exchange activities.

24. While the Committee's guidance uses the term ''bank,'' for purposes of SR-13-24, ''covered institutions'' are those defined in SR-12-17/CA-12-14 as Large Institution Supervision Coordinating Committee (LISCC) firms, large banking organizations (LBOs), and U.S operations of large foreign banking Organizations (large FBOs), as well as any other banking organization that engages in significant foreign exchange activities.

25. The guidance applies to foreign exchange transactions that consist of two settlement payment flows. This includes spot transactions, forwards, swaps, deliverable options, and

- *Guideline 1—Governance.* A bank should have strong governance arrangements over its foreign exchange settlement-related risks, including a comprehensive risk-management process and active engagement by the board of directors.

  Paragraph 3.1.8 of the guidance states that the board of directors of a covered institution should oversee the management of the compliance function associated with settling foreign exchange transactions. For purposes of the application of the guidelines by covered institutions, senior management should routinely communicate significant compliance matters to the board of directors. The board of directors may choose to delegate regular oversight to a single board member or a committee of the board.
- *Guideline 2—Principal risk.* A bank should use financial market infrastructures that provide payment-versus-payment settlement to eliminate principal risk when settling foreign exchange transactions. Where payment-versus-payment settlement is not practicable, a bank should properly identify, measure, control, and reduce the size and duration of its remaining principal risk.
- *Guideline 3—Replacement-cost risk.* A bank should employ prudent risk-mitigation regimes to properly identify, measure, monitor, and control replacement-cost risk for foreign exchange transactions until settlement has been confirmed and reconciled.

  Paragraph 3.3.7 of the guidance refers to transactions with affiliates. Covered institutions are encouraged to exchange variation margin for inter-affiliate transactions as a matter of sound business practice.
- *Guideline 4—Liquidity risk.* A bank should properly identify, measure, monitor, and control its liquidity needs and risks in each currency when settling foreign exchange transactions.
- *Guideline 5—Operational risk.* A bank should properly identify, assess, monitor, and control its operational risks. A bank should ensure that its systems support appropriate risk-management controls, and have sufficient capacity, scalability, and resiliency to handle foreign exchange volumes under normal and stressed conditions.
- *Guideline 6—Legal risk.* A bank should ensure that agreements and contracts are legally enforceable for each aspect of its activities in all relevant jurisdictions.

  Paragraph 3.6.2 of the guidance states that institutions conducting business in multiple jurisdictions should identify, measure, monitor, and control for the risks arising from conflicts of laws across jurisdictions and suggests accomplishing these objectives by obtaining legal opinions from qualified internal or external counsel. The Federal Reserve does not expect a covered institution to obtain a legal opinion for every transaction; rather, management should seek legal advice that addresses standardized terms, master netting and other significant agreements, and individual transactions as appropriate.
- *Guideline 7—Capital for foreign exchange transactions.* When analyzing capital needs, a bank should consider all foreign exchange settlement-related risks, including principal risk and replacement-cost risk. A bank should ensure that sufficient capital is held against these potential exposures, as appropriate.

While the Federal Reserve acknowledges the principles set forth in section 3.7 of the guidance, and in particular that all risks related to the settlement of foreign exchange transactions should be considered in determining capital needs under the applicable capital framework, the guidance does not and is not intended to modify the calculation of regulatory capital requirements for covered institutions.

currency swaps involving exchange of principal. It excludes instruments that involve one-way settlement payments, such as non-deliverable forwards, non-deliverable options, and contracts for difference. The Federal Reserve expects that the guidance will be applied broadly by the covered institutions and notes that there may be limited instances in which an institution need not apply this guidance to an insignificant currency exposure.

Banking organizations have greatly expanded the scope, complexity, and global nature of their business activities. At the same time, compliance requirements associated with these activities have become more complex. As a result, organizations have confronted significant risk management and corporate governance challenges, particularly with respect to compliance risks that transcend business lines, legal entities, and jurisdictions of operation.[1] To address these challenges, many banking organizations have implemented or enhanced firmwide compliance risk-management programs and program oversight.

While the guiding principles of sound risk management are the same for compliance as for other types of risk, the management and oversight of compliance risk presents certain challenges. For example, quantitative limits reflecting the firm's risk appetite can be established for market and credit risks, allocated to the various business lines within the organization, and monitored by units independent of the business line. Compliance risk does not lend itself to similar processes for establishing and allocating overall risk tolerance, in part because organizations must comply with applicable rules and standards. Additionally, existing compliance risk metrics are often less meaningful in terms of aggregation and trend analysis as compared with more traditional market- and credit-risk metrics. These distinguishing characteristics of compliance risk underscore the need for a firmwide approach to compliance risk management and oversight for large, complex organizations. A firmwide compliance function that plays a key role in managing and overseeing compliance risk while promoting a strong culture of compliance across the organization is particularly important for large, complex organizations that have a number of separate business lines and legal entities that must comply with a wide range of applicable rules and standards.

The Federal Reserve strongly encourages large banking organizations with complex compliance profiles to ensure that the necessary resources are dedicated to fully implementing effective firmwide compliance risk-management programs and oversight in a timely manner.[2]

The Federal Reserve's expectations for all supervised banking organizations are consistent with the principles outlined in a paper issued in April 2005 by the Basel Committee on Banking Supervision, entitled *Compliance and the compliance function in banks* (Basel compliance paper). The principles in the Basel compliance paper have become widely recognized as global sound practices for compliance risk management and oversight, and the Federal Reserve endorses these principles. This section provides clarification as to the Federal Reserve's views regarding certain compliance risk management and oversight matters with regard to banking organizations with complex compliance profiles in the specific areas addressed within this section (see SR-08-8/CA-08-11):

1. organizations that should implement a firmwide approach to compliance risk management and oversight;
2. independence of compliance staff;
3. compliance monitoring and testing; and
4. responsibilities of boards of directors and senior management regarding compliance risk management and oversight.

2124.07.1 FIRMWIDE COMPLIANCE RISK MANAGEMENT AND OVERSIGHT

2124.07.1.1 Overview

Organizations supervised by the Federal Reserve, regardless of size and complexity, should have effective compliance risk-management programs that are appropriately tailored to the organizations' risk profiles.[3] The

1. Compliance risk is the risk of legal or regulatory sanctions, financial loss, or damage to reputation resulting from failure to comply with laws, regulations, rules, other regulatory requirements, or codes of conduct and other standards of self-regulatory organizations applicable to the banking organization (applicable rules and standards). (See, generally, *Compliance and the compliance function in banks*, Basel Committee on Banking Supervision, April 2005, www.bis.org.)

2. Effective compliance risk-management programs incorporate controls designed to maintain compliance with applicable rules and standards, including safety and soundness and consumer protection guidance issued by supervisory authorities.

3. See SR-95-51, "Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies." This letter provides general guidance on risk-management processes and internal controls for consolidated organizations and discusses the elements of a sound risk-management system. SR-95-51 states that bank

manner in which the program is implemented and the type of oversight needed for that program can vary considerably, depending upon the scope and complexity of the organization's activities, the geographic reach of the organization, and other inherent risk factors. Larger, more complex banking organizations tend to conduct a wide range of business activities that are subject to complex compliance requirements that frequently transcend business lines and legal entities and, accordingly, present risk-management and corporate governance challenges. Consequently, these organizations typically require a firmwide approach to compliance risk management and oversight that includes a corporate compliance function. In contrast, smaller, less-complex banking organizations are not generally confronted with the types of compliance risks and challenges that require a comprehensive firmwide approach to effectively manage and oversee compliance risk. The following discussion, therefore, is *not* directed at smaller, less-complex banking organizations.

Firmwide compliance risk management refers to the processes established to manage compliance risk across an entire organization, both within and across business lines, support units, legal entities, and jurisdictions of operation. This approach ensures that compliance risk management is conducted in a context broader than would take place solely within individual business lines or legal entities. The need for a firmwide approach to compliance risk management at larger, more complex banking organizations is well demonstrated in areas such as anti-money-laundering, privacy, affiliate transactions, conflicts of interest, and fair lending, where legal and regulatory requirements may apply to multiple business lines or legal entities within the banking organization. Certain other compliance risks may also warrant a firmwide risk-management approach to address similar rules and standards that apply to the organization's operations across different jurisdictions. In all such instances, compliance risk management benefits from an aggregate view of the organization's compliance risk exposure and an integrated approach to managing those risks.

The processes established for managing compliance risk on a firmwide basis should be formalized in a compliance *program* that establishes the framework for identifying, assessing, controlling, measuring, monitoring, and reporting compliance risks across the organization, and for providing compliance training throughout the organization. A banking organization's compliance risk-management program should be documented in the form of compliance policies and procedures and compliance risk-management standards.[4]

Firmwide compliance oversight refers to the processes established to oversee compliance risk management across the entire organization, both within and across business lines, legal entities, and jurisdictions of operation. In larger, more complex banking organizations, a key component of firmwide compliance oversight is a corporate compliance function that has day-to-day responsibility for overseeing and supporting the implementation of the organization's firmwide compliance risk-management program, and that plays a key role in controlling compliance risks that transcend business lines, legal entities, and jurisdictions of operation. Board oversight of such functions are often carried out by the board's risk committee or a committee or subcommittee primarily dedicated to oversight of compliance.

holding companies should be able to assess the major risks of the consolidated organization. See also 12 CFR 208, appendix D-1, "Interagency Guidelines Establishing Standards for Safety and Soundness."

4. Compliance policies refer to both (1) firmwide compliance policies that apply to all employees throughout the organization as they conduct their business and support activities and (2) the more detailed, business-specific policies that are further tailored to, and more specifically address, compliance risks inherent in specific business lines and jurisdictions of operation, and apply to employees conducting business and support activities for the specific business line and/or jurisdiction of operation. Compliance procedures refer to the control procedures that are designed to implement compliance policies. Compliance risk-management standards refer to policies and procedures applicable to compliance staff as they fulfill their day-to-day compliance responsibilities. Compliance standards should clearly articulate expectations regarding the processes to be followed in implementing the organization's firmwide compliance risk-management program, including the processes and criteria to be utilized in identifying, assessing, controlling, measuring, monitoring, and reporting compliance risk, and in providing compliance training. Compliance standards should also clearly articulate the roles and responsibilities of the various committees, functions, and staff with compliance support and oversight responsibilities.

2124.07.1.2 Federal Reserve Supervisory Policies on Compliance Risk Management and Oversight

2124.07.1.2.1 Large Banking Organizations with Complex Compliance Profiles

Although balance sheet size is not the defining indication of a banking organization's compliance risk-management needs, experience has demonstrated that banking organizations with $50 billion or more in consolidated total assets typically have multiple legal entities that pose the type of compliance risks and challenges that call for a comprehensive firmwide approach to appropriately control compliance risk and provide effective oversight. Accordingly, such organizations should generally implement firmwide compliance risk-management programs and have a corporate compliance function.

Compliance programs at such organizations should include more robust processes for identifying, assessing, controlling, measuring, monitoring, and reporting compliance risk, and for providing compliance training throughout the organization in order to appropriately control the heightened level and complexity of compliance risk. The corporate compliance function should play a key role in overseeing and supporting the implementation of the compliance risk-management program and in controlling compliance risks that transcend business lines, legal entities, and jurisdictions of operation.[5]

2124.07.1.2.2 Large Banking Organizations with Less-Complex Compliance Profiles

In some instances, banking organizations that meet the $50 billion asset threshold may have few legal entities, may be less complex in nature, and may engage in only a very limited range of business activities. Such organizations may be able to effectively manage and oversee compliance risk without implementing a comprehensive firmwide approach. Alternatively, these organizations may choose to implement a firmwide approach whose scope is highly risk-focused on particular compliance risks that exist throughout the organization. In lieu of relying on a corporate compliance function to play a key role in providing day-to-day oversight of the compliance program, these organizations may rely on executive and management committees that are actively involved in providing ongoing corporate oversight of the compliance risk-management program. An organization that adopts this approach, however, should ensure that its compliance program incorporates controls that effectively address compliance risks that transcend business lines, legal entities, and jurisdictions of operation; that appropriate firmwide standards are established for the business lines to follow in managing compliance risk and reporting on key compliance matters; and that the organization is appropriately overseeing the implementation of its compliance risk-management program.

2124.07.1.2.3 Foreign Banking Organizations

Each foreign banking organization supervised by the Federal Reserve should implement a compliance program that is appropriately tailored to the scope, complexity, and risk profile of the organization's U.S. operations. The program should be reasonably designed to ensure that the organization's U.S. operations comply with applicable U.S. rules and standards and should establish effective controls over compliance risks that transcend business lines or legal entities. Foreign banking organizations with large, complex U.S. operations should implement compliance programs for these operations that have more robust processes for identifying, assessing, controlling, measuring, monitoring, and reporting compliance risk, and for providing compliance training, than would be appropriate for foreign banking organizations with smaller, less-complex U.S. operations.[6]

5. While the corporate compliance function is generally responsible for overseeing and supporting the compliance risk-management program, it is recognized that the primary responsibility for aspects of the compliance program may be assigned to other units within the organization (e.g., finance, information technology, and human resources). The corporate compliance function, therefore, may or may not have responsibility for monitoring and testing the controls over certain compliance activities embedded within these units, such as those over regulatory reporting and regulatory capital. Nevertheless, it is important that an organization's compliance program incorporates appropriate controls over these risks and that proper oversight of the management of these risks is conducted.

6. Foreign banking organizations with $50 billion or more in U.S. third-party assets will generally be considered as large banking organizations with complex compliance profiles for purposes of SR-08-8/CA-08-1, unless their U.S. activities are less complex in nature as described in subsection 2124.07.1. The Federal Reserve's views on compliance risk-management

With respect to oversight, foreign banking organizations should provide effective oversight of compliance risks within their U.S. operations, including risks that transcend business lines or legal entities. A foreign banking organization, however, has flexibility in organizing its oversight structure. Compliance oversight of U.S. activities may be conducted in a manner that is consistent with the foreign banking organization's broader compliance risk-management framework. Alternatively, a separate function may be established specifically to provide compliance oversight of the organization's U.S. operations. Regardless of the oversight structure utilized by a foreign banking organization, its established oversight mechanisms, governing policies and procedures, and supporting infrastructure for its U.S. operations should be sufficiently transparent for the Federal Reserve to assess their adequacy.

2124.07.2 INDEPENDENCE OF COMPLIANCE STAFF

Federal Reserve supervisory findings at large, complex banking organizations consistently reinforce the need for compliance staff to be appropriately independent of the business lines for which they have compliance responsibilities. Compliance independence facilitates objectivity and avoids inherent conflicts of interest that may hinder the effective implementation of a compliance program. A particular challenge for many organizations is attaining an appropriate level of independence with respect to compliance staff operating within the business lines.

The Federal Reserve does not prescribe a particular organizational structure for the compliance function. Large banking organizations with complex compliance profiles are encouraged, however, to avoid inherent conflicts of interest by ensuring that accountability exists between the corporate compliance function and compliance staff within the business lines. Such accountability would provide the corporate compliance function with ultimate authority regarding the handling of compliance matters, personnel decisions, and actions relating to compliance staff, including retaining control over the budget for, and remuneration of, all compliance staff.[7] Compliance independence should not, however, preclude compliance staff from working closely with the management and staff of the various business lines. To the contrary, compliance functions are generally more effective when strong working relationships between compliance and business line staff exist.

The Federal Reserve recognizes, however, that many large, complex banking organizations have chosen to implement an organizational structure in which compliance staff within a business line have a reporting line into the management of the business. In these circumstances, compliance staff should also have a reporting line through to the corporate compliance function with respect to compliance responsibilities. In addition, a banking organization that chooses to implement such a dual reporting structure should ensure that the following minimum standards are observed in order to minimize potential conflicts of interest associated with this approach:

1. In organizations with dual reporting-line structures, the corporate compliance function should play a key role in determining how compliance matters are handled and in personnel decisions and actions (including remuneration) affecting business-line compliance and local compliance staff, particularly senior compliance staff. Furthermore, the organization should have in place a process designed to ensure that disputes between the corporate compliance function and business-line management regarding compliance matters are resolved objectively. Under such a process, the final decision-making authority should rest either with the corporate compliance function or with a member or committee of senior management that has no business-line responsibilities.
2. Compensation and incentive programs should be carefully structured to avoid undermining the independence of compliance staff. Compliance staff should not be compensated on the basis of the financial performance of the business line. Such an arrangement creates an improper conflict of interest.
3. Banking organizations with dual reporting-line structures should implement appropriate controls and enhanced corporate oversight to identify and address issues that may arise from conflicts of interest affecting compli-

programs apply equally to the large, complex U.S. operations of foreign banking organizations.

7. The reference to all compliance staff includes corporate, business-line, and local compliance staff.

ance staff within the business lines. For example, in these circumstances, the process for providing corporate oversight of monitoring and testing activities performed by compliance staff within the business lines should be especially robust.

2124.07.3 COMPLIANCE MONITORING AND TESTING

Robust compliance monitoring and testing play a key role in identifying weaknesses in existing compliance risk-management controls and are, therefore, critical components of an effective firmwide compliance risk-management program.

2124.07.3.1 Risk Assessments and Monitoring and Testing Programs

Risk assessments are the foundation of an effective compliance monitoring and testing program. The scope and frequency of compliance monitoring and testing activities should be a function of a comprehensive assessment of the overall compliance risk associated with a particular business activity.[8] Large complex banking organizations should ensure that comprehensive risk-assessment methodologies are developed and fully implemented, and that compliance monitoring and testing activities are based upon the resulting risk assessments.

2124.07.3.2 Testing

Compliance testing is necessary to validate (1) that key assumptions, data sources, and procedures utilized in measuring and monitoring compliance risk can be relied upon on an ongoing basis and (2) in the case of transaction testing, that controls are working as intended. The testing of controls and remediation of deficiencies identified as a result of testing activities are essential to maintaining an effective internal control framework.

The scope and frequency of compliance testing activities should be based upon the assessment of the specific compliance risks associated with a particular business activity. Periodic testing of compliance controls by compliance staff is strongly encouraged as this practice tends to result in an enhanced level of compliance testing. If, however, compliance testing is performed exclusively by the internal audit function, particular care should be taken to ensure that high-risk compliance elements are not otherwise obscured by a lower overall risk rating of a broadly defined audit entity. Otherwise, the scope and frequency of audit coverage of higher-risk compliance elements tend to be insufficient.

2124.07.4 RESPONSIBILITIES OF THE BOARD OF DIRECTORS AND SENIOR MANAGEMENT

The primary responsibility for complying with applicable rules and standards rests with the individuals within the organization as they conduct their day-to-day business and support activities. Under the board's oversight, senior management, and the corporate compliance function are responsible for establishing and implementing a comprehensive and effective compliance risk-management program and oversight framework that is reasonably designed to prevent and detect compliance breaches and issues.

To achieve its objectives, a sound and effective firmwide compliance risk-management program should have the support of both the board and senior management. Both board and management should encourage ethical conduct and compliance with applicable rules and standards through the firm's culture. A strong compliance culture reinforces the principle that an organization must conduct its activities in accordance with applicable rules and standards, and encourages employees to conduct all activities in accordance with both the letter and the spirit of applicable rules and standards.

As set forth in applicable law and supervisory guidance, the board and senior management of a banking organization have different, but complementary, roles with respect to compliance risk.[9] The following discussion is intended to clarify existing Federal Reserve supervisory

8. Risk assessments should be based upon firmwide standards that establish the method for, and criteria to be utilized in, assessing risk throughout the organization. Risk assessments should take into consideration both the risk inherent in the activity and the strength and effectiveness of controls designed to mitigate the risk.

9. See, for example, the Basel compliance paper; SR-19-4/CA-19-3, "Supervisory Rating System for Holding Companies with Total Consolidated Assets Less Than $100 Billion"; and SR-95-51, "Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies"; and the United States Sentencing

views with regard to responsibilities of the board related to compliance risk management and oversight, and to differentiate these responsibilities from those of senior management.

2124.07.4.1 Boards of Directors

The board should oversee the development of, review, approve, and periodically monitor the firm's compliance strategy and its alignment with the overall strategy of the firm.[10] The board should direct senior management on the board's information needs regarding the types of compliance risks to which the organization is exposed, any significant compliance matters, and the effectiveness of the compliance risk-management program. The board should oversee and hold senior management accountable for the effective implementation of the compliance risk-management program and for the appropriate and timely resolution of compliance issues. The board should hold senior management accountable for the implementation of performance management and compensation programs that promote sound risk management, compliance with laws, regulations, and internal standards, including for conduct.

The board should promote the stature and independence of the corporate compliance function within the organization and provide the appropriate level of resources to conduct their activities effectively.

2124.07.4.2 Senior Management

Senior management is responsible for communicating, implementing, and reinforcing the organization's compliance culture. Senior management also should implement and enforce the compliance policies and compliance risk-management standards. Senior management of the corporate compliance function should establish, support, and oversee the organization's compliance risk-management program. The corporate compliance function should report to the board, or a committee thereof, on significant compliance matters and the effectiveness of the compliance risk-management program.

Senior management should be fully capable, qualified, and properly motivated to manage the compliance risks arising from the organization's business activities. Senior management should communicate the importance of compliance across, and at all levels of, the organization through ongoing training and other means. Under board oversight, senior management should establish appropriate incentives to integrate compliance objectives into the management goals and compensation structure across the organization, and implement appropriate disciplinary actions and other measures for serious compliance and compliance risk-management failures. Senior management within the corporate compliance function and senior compliance personnel within individual business lines should have the appropriate authority, independence, and access to personnel and information within the organization, and appropriate resources to conduct their activities effectively.

Senior management of a foreign banking organization's U.S. operations should provide sufficient information to governance or control functions in its home country and should ensure that responsible senior management, including in the home country, maintain a thorough understanding of the risk and control environment governing U.S. operations. U.S. management should assess the effectiveness of established governance and control mechanisms on an ongoing basis, including processes for reporting and escalating areas of concern and implementation of corrective action as necessary.

Commission's *Federal Sentencing Guidelines Manual*, chapter eight, "Sentencing of Organizations."

10. Foreign banking organizations should ensure that, with respect to their U.S. operations, the responsibilities of the board described in this section are fulfilled in an appropriate manner through their oversight structure and risk-management framework.

The Federal Reserve utilizes risk-focused supervision frameworks for the various supervisory portfolios, based on the asset size of an institution. These frameworks incorporate a methodology to assess an organization's risks and business activities and to tailor supervisory activities to its risk profile. These frameworks aim to sharpen the focus of supervisory activities on areas that pose the greatest risk to the safety and soundness of banking organizations and on management processes to identify, measure, monitor, and control risks.[1]

The Federal Reserve recognizes that the use of information technology can greatly affect a banking organization's financial condition and operating performance.[2] With the dependency of banking organizations on the use of information technology, the Federal Reserve expects an organization's board of directors to oversee and senior management to effectively manage the risks associated with information technology. Accordingly, examiners must consider the risks associated with information technology in their evaluations of an organization's significant business activities and assess the effectiveness of the risk-management process that the organization applies to information technology. See SR-98-9, "Assessment of Information Technology in the Risk-Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations."

This manual section provides additional guidance for examiners on supervisory objectives—

1. highlighting the critical dependence of the financial services industry on information technology and its potential effect on safety and soundness,
2. reinforcing the concept that the risk-focused supervisory process and related products (risk assessments, supervisory plans, and scope memoranda) for an organization should address the risks associated with its use of information technology,[3] and
3. providing a basic framework and a common vocabulary to evaluate the effectiveness of processes used to manage the risks associated with information technology.

2124.1.1 CHANGING ROLE OF INFORMATION TECHNOLOGY

Financial institutions' use of information technology has evolved over time from the automation of routine transactions and preparation of financial reports to the use of artificial intelligence and online banking services. Some decision-making processes such as credit scoring and securities trading have been fully automated. Complex financial products also rely on technology because of the great use of valuation models. Moreover, technological advances in communications and connectivity have minimized geographic constraints within the industry.

While information technology enables banking organizations to carry out their activities more efficiently and effectively, information technology also can be a source of risk to the industry. The operational concerns associated with information processing, traditionally the domain of the "back office," have assumed critical importance during banking mergers and consolidations.

Banking organizations, recognizing the dependency of their operations and decision-making processes on efficient and effective use of information technology, devote significant resources to the management of their information technology resources. In large banking organizations, the positions of the chief information officer and chief technology officer have become more visible executives. In addition, managers of activities that rely on end-user computing and distributed processing systems have been assigned more direct responsibility for the information technology used in their activities. As a result, the management of the risks associated with information technology

1. The types of risk may be categorized according to those presented in the guidelines for rating risk management (that is, credit, market, liquidity, operational, legal, and reputational) or by categories defined by the institution or other supervisory agencies. If the institution uses risk categories that differ from those defined by the supervisory agencies, those categories may be used if all relevant types of risks are captured. See SR-95-51, "Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies."

2. Information technology refers to a business resource that is the combination of computers (hardware and software), telecommunications, and information.

3. Refer to the FFIEC IT Examination Handbook Infobase at: https://ithandbook.ffiec.gov.

should be evaluated for each significant business activity as well as for the overall organization.

Notwithstanding the move towards decentralized management of information technology, large centralized computer systems are still an integral part of the information technology on which many large banking organizations rely. This includes systems critical to the access to payments systems platforms and to the transfer and custody of securities. Similarly, with the continued growth of outsourcing, many third-party information technology service centers also perform a vital role in the banking industry. Therefore, the supervisory review of the effectiveness and reliability of the critical management information systems and third-party processors will continue to be included in the Federal Reserve's supervisory review of a firm's operational resiliency.

2124.1.2 IMPLICATIONS FOR RISK-FOCUSED SUPERVISION

The risk-focused supervisory process evolves and adapts in response to the changing role of information technology in firms' operations, with a greater emphasis being placed on an evaluation of the adequacy of a firm's information technology resources and an assessment of a firm's operational resiliency and risks to its safety and soundness. Accordingly, examiners consider information technology when developing their risk assessments and supervisory plans. Examiners are expected to exercise appropriate judgment in determining the level of review, given the characteristics, size, and business activities of the organization. Moreover, to determine the scope of supervisory activities, the general safety-and-soundness examiners and information technology specialists coordinate their risk assessment, supervisory plan, and scope of the examination or inspection. In general, examiners will

1. Develop a broad understanding of the organization's approach, strategy, and structure with regard to information technology. This requires a determination of the role and importance of information technology to the organization and any unique characteristics or issues.
2. Incorporate an analysis of information technology systems into risk assessments, supervisory plans, and scope memoranda. The analysis should include identification of critical information technology systems, related management responsibility, and the major technology components. An organization's information technology systems should be considered in relation to the size, activities, and complexity of the organization, as well as the degree of reliance on these systems.
3. Assess the organization's critical systems, that is, those that support its major business activities, and the degree of reliance those activities have on information technology systems. The level of review should be sufficient to determine that the systems are delivering the services necessary for the organization to conduct its business safely and soundly.
4. Determine whether senior management is adequately identifying, measuring, monitoring, and controlling the significant risks associated with information technology for the overall organization and its major business activities.

2124.1.3 FRAMEWORK FOR EVALUATING INFORMATION TECHNOLOGY

In order to provide a common terminology and consistent approach for evaluating the adequacy of an organization's information technology, five information technology elements are introduced and defined below. These elements may be used to evaluate the information technology processes at the functional business level or for the organization as a whole. They may also be applied to a variety of information technology management structures: centralized, decentralized, or outsourced.[4]

Although deficiencies in information technology appear to be most directly related to operational risk, information technology also can affect the other business risks (credit, market, liquidity, legal, and reputational), depending on the specific circumstances. Examiners should view the information technology elements in an integrated manner with the overall business risks of the organization or business activity; a deficiency in any one of these five elements could have a substantive adverse effect on the organization's or an activity's business risks.

4. When banking organizations outsource operations, they delegate a certain level of responsibility and authority to an outside party (depending on the contractual arrangements). However, ultimate accountability remains with the banking organization.

Moreover, the elements below do not replace or independently add to the business risks described in SR-95-51. Rather, these elements should be assessed in relation to all of the organization's business risks.

These elements are to be used as a flexible tool to facilitate discussion between the organization and examiners about the risks associated with information technology. Where an organization uses different terminology to describe information technology elements, examiners may use the organization's terminology provided the organization adequately addresses the five elements discussed below. Regardless of the terminology employed, examiners should focus on those systems and issues that are considered critical to the organization.

The five information technology elements are

1. *Management processes*. Management processes[5] encompass planning, investment, development, execution, and staffing of information technology from a corporate-wide and business-specific perspective. Management processes over information technology are effective when they are adequately and appropriately aligned with, and supportive of, the organization's mission and business objectives. Management processes include strategic planning, management and reporting hierarchy, management succession, and a regular independent review function. Examiners should determine if the information technology strategy for the business activity or organization is consistent with the organization's mission and business objectives and whether the information technology function has effective management processes to execute that strategy.
2. *Architecture*. Architecture[6] refers to the underlying design of an automated information system and its individual components. The underlying design encompasses both physical and logical architecture, including operating environments, as well as the organization of data. The individual components refer to network communications, hardware, and software, which includes operating systems, communications software, database management systems, programming languages, and desktop software. Effective architecture meets current and long-term organizational objectives, addresses capacity requirements to ensure that systems allow users to easily enter data at both normal and peak processing times, and provides satisfactory solutions to problems that arise when information is stored and processed in two or more systems that cannot be connected electronically. In assessing the adequacy of information technology architecture, examiners should consider the hardware's capability to run the software, the compatibility and integration with other systems and sources of data, the ability to upgrade to higher levels of performance and capacity, and the adequacy of controls.
3. *Integrity*. Integrity refers to the reliability, accuracy, and completeness of information delivered to the end-user. An information technology system has an effective level of integrity when the resulting information flows are accurate and complete. Insufficient integrity in an organization's systems could adversely affect day-to-day reliability, processing performance, input and output accuracy, and the ease of use of critical information. Examiners should review and consider whether the organization relies upon information system audits or independent application reviews to ensure the integrity of its systems. To assess the integrity of an organization's systems, examiners should review the reliability, accuracy, and completeness of information delivered.
4. *Security*. Security refers to the safety afforded to information assets and their data processing environments, using both physical and logical controls to achieve a level of protection commensurate with the value of the assets. Information technology has effective security when controls prevent unauthorized access; modification; destruction; or disclosure of information assets during their creation, transmission, processing, maintenance, or storage. Examiners should ensure that operating procedures and controls are commensurate with the potential for and risks associated with security breaches, which may be either physical or electronic, inadvertent or intentional, or internal or external.
5. *Availability*. Availability refers to the delivery of information to end-users. Information technology has effective availability when information is consistently delivered on a timely basis in support of business and decision-making processes. In assessing the adequacy of availability, examiners should consider the capability of information tech-

5. Also referred to as "organization" or "strategic."
6. Sometimes referred to as "infrastructure."

nology to provide information from either primary or secondary sources to the end-users, as well as the ability of back-up systems, presented in contingency plans, to mitigate business disruption. Contingency plans should set out a process for an organization to restore or replace its information-processing resources, reconstruct its information assets, and resume its business activity from disruption caused by human error or intervention, natural disaster, or infrastructure failure (including the loss of utilities and communication lines and operational failure of hardware, software, and network communications).

Appendix A provides a table with examples of situations where deficiencies in information technology elements potentially have a negative effect on the business risks of an organization. The table also provides possible actions that an organization could take in these situations to mitigate its risks. The examples in this table are representative and should not be viewed as an exhaustive list of the risks associated with information technology.

2124.1.4 ALIGNING EXAMINER STAFFING WITH THE TECHNOLOGY ENVIRONMENT

Complex computer systems are an integral part of the information technology for large organizations. Information technology processes have become embedded in the various business activities of a banking organization—particularly with the increased use of local area networks and personal computers. Many community and regional banks continue to rely on third-party information technology service providers. Therefore, the level of technical expertise needed for a particular examination or inspection will vary and should be identified during examination planning. For example, a specialist in information technology or the particular business activity may be the most appropriate person to review an institution's information technology integrity, while general safety-and-soundness examiners may be better suited to review management processes related to information technology.

Development of the overall supervisory approach for an organization requires collaboration between general safety-and-soundness examiners and information technology specialists. Accordingly, a discussion of information technology should be integrated into the supervisory process and products. That is, examiners should consider and comment on the risks associated with information technology when developing an understanding of an organization, assessing an organization's risks, and preparing a scope memorandum.

Appendix A—Examples of Information Technology Elements that Should Be Considered in Assessing Business Risks of Particular Situations

Situation	*IT elements to be considered*	*Potential effect on business risks*	*Risk mitigants*
A bank holding company expands very rapidly via acquisition into new product lines and geographic areas.	*Management processes.* Lack of clear, cohesive strategies could result in dependence on different systems that are incompatible and fragmented. *Integrity.* Unreliable information could be produced due to incompatible systems. *Availability.* Critical information may not be available to management when needed.	*Credit risk.* Exposure to less creditworthy borrowers may increase. *Liquidity risk.* Depositors may withdraw funds or close accounts due to unreliable account information. *Operational risk.* Controls may be inadequate to address the increase in manual interventions to correct incompatibility problems between affiliates' systems, leading to a greater potential for fraudulent transactions.	Develop a well-thought-out plan for integrating acquired systems, mapping data flows and sources, and ensuring reliability of systems.
A bank's consumer loan division inputs erroneous entries into the general-ledger system.	*Integrity.* Billing errors and unwarranted late-payment fees could occur due to the inaccurate loan information maintained by the system.	*Reputational risk.* Knowledge of errors could become widespread resulting in adverse public opinion. *Operational risk.* Increased expenditures may be required to resolve accounting operations problems. *Legal risk.* Litigation could arise because of errors in customer accounts due to processing deficiencies.	Improve policies and procedures related to input of accounting entries. Ensure internal audit considers system aspects of accounting operations.
Substantial turnover occurs in bank's wire-transfer department.	*Security.* Security procedures could be compromised due to inadequate training and lack of qualified personnel. *Integrity.* System may not be able to provide "real-time" funds availability.	*Operational risk.* Financial losses could occur due to fraud or incorrectly sent wire transfers. *Legal risk.* Litigation could arise as a result of errors in customer accounts and fraudulent wire transfers. *Reputational risk.* Knowledge of fraudulent or erroneous wire operations could result in adverse public opinion.	Increase and strengthen procedural and access controls for wire operations. Implement security measures such as passwords and firewalls. Develop and monitor appropriate audit trails. Provide for adequate training program and staffing levels.

The Federal Reserve issued this guidance to assist financial institutions in understanding and managing the risks associated with outsourcing a bank activity to a service provider to perform that activity. Refer to SR-13-19/CA-13-21, "Guidance on Managing Outsourcing Risk."

In addition to traditional core bank processing and information technology services, financial institutions outsource operational activities such as accounting, appraisal management, internal audit, human resources, sales and marketing, loan review, asset and wealth management, procurement, and loan servicing.[1] The Federal Reserve has issued this guidance to financial institutions to highlight the potential risks that arise from the use of service providers and to describe the elements of an appropriate service provider risk-management program. This guidance supplements existing guidance on technology service provider risk,[2] and applies to service provider relationships where business functions or activities are outsourced. For purposes of this guidance, "service providers" is broadly defined to include all entities that have entered into a contractual relationship with a financial institution to provide business functions or activities.[3]

2124.3.1 RISKS FROM THE USE OF SERVICE PROVIDERS

The use of service providers to perform operational functions presents various risks to financial institutions. Some risks are inherent to the outsourced activity itself, whereas others are introduced with the involvement of a service provider. If not managed effectively, the use of service providers may expose financial institutions to risks that can result in regulatory action, financial loss, litigation, and loss of reputation. Financial institutions should consider the following risks before entering into and while managing outsourcing arrangements.

- *Compliance risks* arise when the services, products, or activities of a service provider fail to comply with applicable U.S. statutes and regulations.
- *Concentration risks* arise when outsourced services or products are provided by a limited number of service providers or are concentrated in limited geographic locations.
- *Reputational risks* arise when actions or poor performance of a service provider causes the public to form a negative opinion about a financial institution.
- *Country risks* arise when a financial institution engages a foreign-based service provider, exposing the institution to possible economic, social, and political conditions and events from the country where the provider is located.
- *Operational risks* arise when a service provider exposes a financial institution to losses due to inadequate or failed internal processes or systems or from external events and human error.
- *Legal risks* arise when a service provider exposes a financial institution to legal expenses and possible lawsuits.

2124.3.2 ROLE OF SENIOR MANAGEMENT

The use of service providers does not relieve a financial institution of the responsibility to ensure that outsourced activities are conducted in a safe-and-sound manner and in compliance with applicable statutes and regulations. Senior management should establish policies governing the use of service providers that are appropriate for the range and risks of the institution's outsourced activity and organizational structure. These policies should establish a service provider risk management program that addresses risk assessments and due diligence, standards for contract provisions and considerations, ongoing monitoring of service providers, and business continuity and contingency planning.

Senior management is responsible for ensuring that policies for the use of service providers are appropriately executed. This includes overseeing the development and implementation of an appropriate risk-management and reporting framework that includes elements described in this guidance. Senior management is also responsible for providing the institution's board of directors with sufficient information about

1. For purposes of this guidance, a "financial institution" refers to state member banks, bank and savings and loan holding companies (including their nonbank subsidiaries), and U.S. operations of foreign banking organizations.
2. Refer to the FFIEC Outsourcing Technology Services Booklet.
3. Entities may be a bank or nonbank, affiliated or nonaffiliated, regulated or non-regulated, or domestic or foreign.

outsourcing arrangements so that the board can understand the risks posed by these arrangements.

2124.3.3 SERVICE PROVIDER RISK-MANAGEMENT PROGRAMS

A financial institution's service provider risk-management program should be risk-focused and provide oversight and controls commensurate with the level of risk presented by the outsourcing arrangements in which the financial institution is engaged. It should focus on outsourced activities that have a substantial impact on a financial institution's financial condition; are critical to the institution's ongoing operations; involve sensitive customer information or new bank products or services; or pose material compliance risk.

The depth and formality of the service provider risk-management program will depend on the criticality, complexity, and number of material business activities being outsourced. A community banking organization may have critical business activities being outsourced, but the number may be few and to highly reputable service providers. Therefore, the risk-management program may be simpler and use less elements and considerations. For those financial institutions that may use hundreds or thousands of service providers for numerous business activities that have material risk, the financial institutions may find that they need to use many more elements and considerations of a service provider risk-management program to manage the higher level of risk and reliance on service providers.

While the activities necessary to implement an effective service provider risk-management program can vary based on the scope and nature of a financial institution's outsourced activities, effective programs usually include the following core elements:

- risk assessments, due diligence and selection of service providers;
- contract provisions and considerations;
- incentive compensation review;
- oversight and monitoring of service providers; and
- business continuity and contingency plans.

A. Risk Assessments

Risk assessment of a business activity and the implications of performing the activity in-house or having the activity performed by a service provider are fundamental to the decision of whether or not to outsource. A financial institution should determine whether outsourcing an activity is consistent with the strategic direction and overall business strategy of the organization. After that determination is made, a financial institution should analyze the benefits and risks of outsourcing the proposed activity as well as the service provider risk, and determine cost implications for establishing the outsourcing arrangement. Consideration should also be given to the availability of qualified and experienced service providers to perform the service on an ongoing basis. Additionally, management should consider the financial institution's ability and expertise to provide appropriate oversight and management of the relationship with the service provider.

This risk assessment should be updated at appropriate intervals consistent with the financial institution's service provider risk-management program. A financial institution should revise its risk mitigation plans, if appropriate, based on the results of the updated risk assessment.

B. Due Diligence and Selections of Service Providers

A financial institution should conduct an evaluation of and perform the necessary due diligence for a prospective service provider prior to engaging the service provider. The depth and formality of the due diligence performed will vary depending on the scope, complexity, and importance of the planned outsourcing arrangement, the financial institution's familiarity with prospective service providers, and the reputation and industry standing of the service provider. Throughout the due diligence process, financial institution technical experts and key stakeholders should be engaged in the review and approval process as needed. The overall due diligence process includes a review of the service provider with regard to business background, reputation, and strategy; financial performance and condition; and operations and internal controls.

1. Business Background, Reputation, and Strategy

Financial institutions should review a prospective service provider's status in the industry and corporate history and qualifications; review the background and reputation of the service provider and its principals; and ensure that the service provider has an appropriate background check program for its employees.

The service provider's experience in providing the proposed service should be evaluated in order to assess its qualifications and competencies to perform the service. The service provider's business model, including its business strategy and mission, service philosophy, quality initiatives, and organizational policies should be evaluated. Financial institutions should also consider the resiliency and adaptability of the service provider's business model as factors in assessing the future viability of the provider to perform services.

Financial institutions should check the service provider's references to ascertain its performance record, and verify any required licenses and certifications. Financial institutions should also verify whether there are any pending legal or regulatory compliance issues (for example, litigation, regulatory actions, or complaints) that are associated with the prospective service provider and its principals.

2. Financial Performance and Condition

Financial institutions should review the financial condition of the service provider and its closely related affiliates. The financial review may include:

- The service provider's most recent financial statements and annual report with regard to outstanding commitments, capital strength, liquidity, and operating results.
- The service provider's sustainability, including factors such as the length of time that the service provider has been in business and the service provider's growth of market share for a given service.
- The potential impact of the financial institution's business relationship on the service provider's financial condition.
- The service provider's commitment (both in terms of financial and staff resources) to provide the contracted services to the financial institution for the duration of the contract.
- The adequacy of the service provider's insurance coverage.
- The adequacy of the service provider's review of the financial condition of any subcontractors.
- Other current issues the service provider may be facing that could affect future financial performance.

3. Operations and Internal Controls

Financial institutions are responsible for ensuring that services provided by service providers comply with applicable statutes and regulations and are consistent with safe-and-sound banking practices. Financial institutions should evaluate the adequacy of standards, policies, and procedures. Depending on the characteristics of the outsourced activity, some or all of the following may need to be reviewed:

1. internal controls;
2. facilities management (such as access requirements or sharing of facilities);
3. training, including compliance training for staff;
4. security of systems (for example, data and equipment);
5. privacy protection of the financial institution's confidential information;
6. maintenance and retention of records;
7. business resumption and contingency planning;
8. systems development and maintenance;
9. service support and delivery;
10. employee background checks; and
11. adherence to applicable laws, regulations, and supervisory guidance.

C. Contract Provisions and Considerations

Financial institutions should understand the service contract and legal issues associated with proposed outsourcing arrangements. The terms of service agreements should be defined in written contracts that have been reviewed by the financial institution's legal counsel prior to execution. The characteristics of the business activity being outsourced and the service provider's strategy for providing those services will determine the terms of the contract. Elements of well-defined contracts and service agreements usually include:

1. *Scope:* Contracts should clearly define the rights and responsibilities of each party, including:
   - support, maintenance, and customer service;
   - contract timeframes;
   - compliance with applicable laws, regulations, and regulatory guidance;
   - training of financial institution employees;
   - the ability to subcontract services;
   - the distribution of any required statements or disclosures to the financial institution's customers;
   - insurance coverage requirements; and
   - terms governing the use of the financial institution's property, equipment, and staff.
2. *Cost and compensation:* Contracts should describe the compensation, variable charges, and any fees to be paid for nonrecurring items and special requests. Agreements should also address which party is responsible for the payment of any legal, audit, and examination fees related to the activity being performed by the service provider. Where applicable, agreements should address the party responsible for the expense, purchasing, and maintenance of any equipment, hardware, software or any other item related to the activity being performed by the service provider. In addition, financial institutions should ensure that any incentives (for example, in the form of variable charges, such as fees and/or commissions) provided in contracts do not provide potential incentives to take imprudent risks on behalf of the institution.
3. *Right to audit:* Agreements may provide for the right of the institution or its representatives to audit the service provider and/or to have access to audit reports. Agreements should define the types of audit reports the financial institution will receive and the frequency of the audits and reports.
4. *Establishment and monitoring of performance standards:* Agreements should define measurable performance standards for the services or products being provided.
5. *Confidentiality and security of information:* Consistent with applicable statutes, regulations, and supervisory guidance, service providers should ensure the security and confidentiality of both the financial institution's confidential information and the financial institution's customer information. Information security measures for outsourced functions should be viewed as if the activity were being performed by the financial institution and afforded the same protections. Financial institutions have a responsibility to ensure service providers take appropriate measures designed to meet the objectives of the information security guidelines within Federal Financial Institutions Examination Council (FFIEC) guidance,[4] as well as comply with section 501(b) of the Gramm-Leach-Bliley Act. These measures should be mapped directly to the security processes at financial institutions, as well as be included or referenced in agreements between financial institutions and service providers.

   Service agreements should also address service provider use of financial institution information and its customer information. Information made available to the service provider should be limited to what is needed to provide the contracted services. Service providers may reveal confidential supervisory information only to the extent authorized under applicable statutes and regulations.[5]

   If service providers handle any of the financial institution customer's Nonpublic Personal Information (NPPI), the service providers must comply with applicable privacy statutes and regulations.[6] Financial institutions should require notification from service providers of any breaches involving the disclosure of NPPI data. Generally, NPPI data is any nonpublic personally identifiable financial information; and any list, description, or other grouping of consumers (and publicly available information pertaining to them) derived using any personally identifiable financial information that is not publicly available.[7] Financial institutions and their service providers who maintain, store, or process NPPI data are responsible for that information and any disclosure of it. The security of, retention of, and access to NPPI data should be addressed in any contracts with service providers.

   When a breach or compromise of NPPI data occurs, financial institutions have legal requirements that vary by state and these requirements should be made part of the

4. For further guidance regarding vendor security practices, refer to the FFIEC Information Security Booklet.
5. See 12 CFR part 261.
6. See 12 CFR part 1016.
7. See 12 U.S.C. 6801(b).

contracts between the financial institution and any service provider that provides storage, processing, or transmission of NPPI data. Misuse or unauthorized disclosure of confidential customer data by service providers may expose financial institutions to liability or action by a federal or state regulatory agency. Contracts should clearly authorize and disclose the roles and responsibilities of financial institutions and service providers regarding NPPI data.

6. *Ownership and license:* Agreements should define the ability and circumstances under which service providers may use financial institution property inclusive of data, hardware, software, and intellectual property. Agreements should address the ownership and control of any information generated by service providers. If financial institutions purchase software from service providers, escrow agreements may be needed to ensure that financial institutions have the ability to access the source code and programs under certain conditions.[8]
7. *Indemnification:* Agreements should provide for service provider indemnification of financial institutions for any claims against financial institutions resulting from the service provider's negligence.
8. *Default and termination:* Agreements should define events of a contractual default, list of acceptable remedies, and provide opportunities for curing default. Agreements should also define termination rights, including change in control, merger or acquisition, increase in fees, failure to meet performance standards, failure to fulfill the contractual obligations, failure to provide required notices, and failure to prevent violations of law, bankruptcy, closure, or insolvency. Contracts should include termination and notification requirements that provide financial institutions with sufficient time to transfer services to another service provider. Agreements should also address a service provider's preservation and timely return of financial institution data, records, and other resources.
9. *Dispute resolution:* Agreements should include a dispute resolution process in order to expedite problem resolution and address the continuation of the arrangement between the parties during the dispute resolution period.
10. *Limits on liability:* Service providers may want to contractually limit their liability. Financial institutions should determine whether the proposed limitations are reasonable when compared to the risks to the institution if a service provider fails to perform.[9]
11. *Insurance:* Service providers should have adequate insurance and provide financial institutions with proof of insurance. Further, service providers should notify financial institutions when there is a material change in their insurance coverage.
12. *Customer complaints:* Agreements should specify the responsibilities of financial institutions and service providers related to responding to customer complaints. If service providers are responsible for customer complaint resolution, agreements should provide for summary reports to the financial institutions that track the status and resolution of complaints.
13. *Business resumption and contingency plan of the service provider:* Agreements should address the continuation of services provided by service providers in the event of operational failures. Agreements should address service provider responsibility for backing up information and maintaining disaster recovery and contingency plans. Agreements may include a service provider's responsibility for testing of plans and providing testing results to financial institutions.
14. *Foreign-based service providers:* For agreements with foreign-based service providers, financial institutions should consider including express choice of law and jurisdictional provisions that would provide for the adjudication of all disputes between the two parties under the laws of a single, specific jurisdiction. Such agreements may be subject to the interpretation of foreign courts relying on local laws. Foreign law may differ from U.S. law in the enforcement of contracts. As a result, financial institutions should seek legal advice regarding the enforceability of all aspects of proposed

8. Escrow agreements are established with vendors when buying or leasing products that have underlying proprietary software. In such agreements, an organization can only access the source program code under specific conditions, such as discontinued product support or financial insolvency of the vendor.

9. Refer to SR-06-4, "Interagency Advisory on the Unsafe and Unsound Use of Limitations on Liability Provisions in External Audit Engagement Letters," regarding restrictions on the liability limitations for external audit engagements or section 2060.1.

contracts with foreign-based service providers and the other legal ramifications of such arrangements.

15. *Subcontracting:* If agreements allow for subcontracting, the same contractual provisions should apply to the subcontractor. Contract provisions should clearly state that the primary service provider has overall accountability for all services that the service provider and its subcontractors provide. Agreements should define the services that may be subcontracted, the service provider's due diligence process for engaging and monitoring subcontractors, and the notification and approval requirements regarding changes to the service provider's subcontractors. Financial institutions should pay special attention to any foreign subcontractors, as information security and data privacy standards may be different in other jurisdictions. Additionally, agreements should include the service provider's process for assessing the subcontractor's financial condition to fulfill contractual obligations.

D. Incentive Compensation Review

Financial institutions should also ensure that an effective process is in place to review and approve any incentive compensation that may be embedded in service provider contracts, including a review of whether existing governance and controls are adequate in light of risks arising from incentive compensation arrangements. As the service provider represents the institution by selling products or services on its behalf, the institution should consider whether the incentives provided might encourage the service provider to take imprudent risks. Inappropriately structured incentives may result in reputational damage, increased litigation, or other risks to the financial institution. An example of an inappropriate incentive would be one where variable fees or commissions encourage the service provider to direct customers to products with higher profit margins without due consideration of whether such products are suitable for the customer.

E. Oversight and Monitoring of Service Providers

To effectively monitor contractual requirements, financial institutions should establish acceptable performance metrics that the business line or relationship management determines to be indicative of acceptable performance levels. Financial institutions should ensure that personnel with oversight and management responsibilities for service providers have the appropriate level of expertise and stature to manage the outsourcing arrangement. The oversight process, including the level and frequency of management reporting, should be risk-focused. Higher risk service providers may require more frequent assessment and monitoring and may require financial institutions to designate individuals or a group as a point of contact for those service providers. Financial institutions should tailor and implement risk mitigation plans for higher risk service providers that may include processes such as additional reporting by the service provider or heightened monitoring by the financial institution. Further, more frequent and stringent monitoring is often necessary for service providers that exhibit performance, financial, compliance, or control concerns. For lower risk service providers, the level of monitoring can be lessened.

Financial condition: Financial institutions should have established procedures to monitor the financial condition of service providers to evaluate their ongoing viability. In performing these assessments, financial institutions should review the most recent financial statements and annual report with regard to outstanding commitments, capital strength, liquidity, and operating results. If a service provider relies significantly on subcontractors to provide services to financial institutions, then the service provider's controls and due diligence regarding the subcontractors should also be reviewed.

Internal controls: For significant service provider relationships, financial institutions should assess the adequacy of the provider's control environment. Assessments should include reviewing available audits or reports such as the American Institute of Certified Public Accountants' Service Organization Control 2 report.[10] If the service provider delivers information technology services, the financial institution can request the FFIEC Technology Service Provider examination report from its primary federal regulator. Security incidents at the service pro-

10. Refer to www.AICPA.org.

vider may also necessitate the institution to elevate its monitoring of the service provider.

Escalation of oversight activities: Financial institutions should ensure that risk-management processes include triggers to escalate oversight and monitoring when service providers are failing to meet performance, compliance, control, or viability expectations. These procedures should include more frequent and stringent monitoring and follow-up on identified issues, on-site control reviews, and when an institution should exercise its right to audit a service provider's adherence to the terms of the agreement. Financial institutions should develop criteria for engaging alternative outsourcing arrangements and terminating the service provider contract in the event that identified issues are not adequately addressed in a timely manner.

F. Business Continuity and Contingency Considerations

Various events may affect a service provider's ability to provide contracted services. For example, services could be disrupted by a provider's performance failure, operational disruption, financial difficulty, or failure of business continuity and contingency plans during operational disruptions or natural disasters. Financial institution contingency plans should focus on critical services provided by service providers and consider alternative arrangements in the event that a service provider is unable to perform.[11] When preparing contingency plans, financial institutions should

- ensure that a disaster recovery and business continuity plan exists with regard to the contracted services and products;
- assess the adequacy and effectiveness of a service provider's disaster recovery and business continuity plan and its alignment to their own plan;
- document the roles and responsibilities for maintaining and testing the service provider's business continuity and contingency plans;
- test the service provider's business continuity and contingency plans on a periodic basis to ensure adequacy and effectiveness; and
- maintain an exit strategy, including a pool of comparable service providers, in the event that a contracted service provider is unable to perform.

11. For further guidance regarding business continuity planning with service providers, refer to the FFIEC Business Continuity Management Booklet.

G. Additional Risk Considerations

Suspicious Activity Report (SAR) reporting functions: The confidentiality of suspicious activity reporting makes the outsourcing of any SAR-related function more complex. Financial institutions need to identify and monitor the risks associated with using service providers to perform certain suspicious activity reporting functions in compliance with the Bank Secrecy Act (BSA). Financial institution management should ensure they understand the risks associated with such an arrangement and any BSA-specific guidance in this area.

Foreign-based service providers: Financial institutions should ensure that foreign-based service providers are in compliance with applicable U.S. laws, regulations, and regulatory guidance. Financial institutions may also want to consider laws and regulations of the foreign-based provider's country or regulatory authority regarding the financial institution's ability to perform on-site review of the service provider's operations. In addition, financial institutions should consider the authority or ability of home country supervisors to gain access to the financial institution's customer information while examining the foreign-based service provider.

Internal audit: Financial institutions should refer to existing guidance on the engagement of independent public accounting firms and other outside professionals to perform work that has been traditionally carried out by internal auditors.[12] The Sarbanes-Oxley Act of 2002 specifically prohibits a registered public accounting firm from performing certain non-audit services for a public company client for whom it performs financial statement audits.

Risk-management activities: Financial institutions may outsource various risk-management activities, such as aspects of interest rate risk and model risk management. Financial institutions should require service providers to provide information that demonstrates developmental evidence explaining the product components, design, and intended use, to determine whether

12. Refer to SR-13-1, "Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing," specifically the section titled, "Depository Institutions Subject to the Annual Audit and Reporting Requirements of Section 36 of the FDI Act." See section 2060.07 of this manual. Refer also to SR-03-5, "Amended Interagency Guidance on the Internal Audit Function and its Outsourcing," particularly the section titled,"Institutions Not Subject to Section 36 of the FDI Act that are Neither Public Companies nor Subsidiaries of Public Companies." See section 2060.05 of this manual.

the products and/or services are appropriate for the institution's exposures and risks.[13] Financial institutions should also have standards and processes in place for ensuring that service providers offering model risk-management services, such as validation, do so in a way that is consistent with existing model risk-management guidance.

13. Refer to SR-11-7, "Guidance on Model Risk Management" or section 2126.0 which informs financial institutions of the importance and risk to the use of models and the supervisory expectations that financial institutions should adhere to.

WHAT'S NEW IN THIS REVISED SECTION

Effective July 2012, this section was revised to remove references to SR-97-32, "Sound Practices Guidance for Information Security Networks" and SR-00-4, "Outsourcing of Information and Transaction Processing," which were deemed inactive by SR-12-6. A reference to inactive SR-03-12, "Revisions to the Suspicious Activity Report Form," was also removed.

2124.4.1 INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS

The federal banking agencies jointly issued interagency guidelines establishing information security standards (the information security standards), which became effective July 1, 2001.[1] (See appendix A, section 2124.4.5.) The Board of Governors of the Federal Reserve System approved amendments to the standards on December 16, 2004 (effective July 1, 2005). The amended information security standards implement sections of 501 and 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805) and section 216 of the Fair and Accurate Credit Transactions Act of 2003 (15 U.S.C. 1681w). The Gramm-Leach-Bliley Act requires the agencies to establish information standards consisting of administrative, technical, and physical safeguards for customer records and information. (See SR-01-15.) Bank holding companies and financial holding companies must comply with the information security standards (see appendix F for Regulation Y).[2] The information security standards apply to customer information maintained by or on behalf of state member banks, bank holding companies, and the nonbank subsidiaries or affiliates of each.[3] The information security standards include standards for the proper disposal of consumer and customer information and guidance on response programs for unauthorized access to customer information. (See SR-05-23/CA-05-10.) See sections 2124.4.1.1 and 2124.4.2.

Under the information security standards, each bank holding company falling within the scope of the standards must implement a comprehensive, written information security program.[4] A bank holding company's board of directors, or an appropriate committee of the board, must oversee the company's development, implementation, and maintenance of the information security program—this board oversight includes assigning specific responsibility for the program's implementation and reviewing reports received from management. The information security program should include administrative, technical, and physical safeguards appropriate to the size and complexity of the bank holding company and the nature and scope of its activities.

While all parts of a bank holding company are not required to implement a uniform information security program and set of policies, all elements of the information security program must be coordinated. A bank holding company must ensure that each of its subsidiaries is subject to a comprehensive information security program. It may fulfill this requirement either 1) by including a subsidiary within the scope of the bank's holding company's comprehensive information security program or (2) by having the subsidiary implement a separate comprehensive information security program in accordance with the information security standards and procedures of appendix F, Regulation Y.

A bank holding company's information security program must be designed to (1) ensure the security and confidentiality of customer information,[5] (2) protect against anticipated threats

1. The 2001 information security standards were titled Interagency Guidelines Establishing Standards for Safeguarding Customer Information. See 66 *Fed. Reg.* 8,616–8,641 (February 1, 2001); 69 *Fed. Reg.* 7,610–7,621 (December 28, 2004); and Regulation H, 12 CFR 208, appendix D-2; Regulation K, 12 CFR 211.9 and 211.24; and Regulation Y, 12 CFR 225, appendix F.

2. The discussion in this section applies equally to financial holding companies and bank holding companies.

3. The information security standards do not apply to brokers, dealers, investment companies, and investment advisers, or to persons providing insurance under the applicable state insurance authority of the state in which the person is domiciled. The appropriate federal agency or state insurance authority regulates these insurance entities under sections 501 and 505 of the Gramm-Leach-Bliley Act.

4. The information security standards apply to customer information; as a result, a bank holding company that does not maintain any customer information is not subject to the information security standards. In addition, when customer information is maintained only in the banking subsidiaries or functionally regulated nonbank subsidiaries of the holding company, examiners generally may rely on the primary supervisor's assessment of the subsidiaries' information security programs, if applicable, to determine the holding company's compliance with the information security standards.

5. *Customer information* is defined to include any record, whether in paper, electronic, or other form, containing *non-*

or hazards to the security or integrity of such information, (3) protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer, and (4) ensure the proper disposal of customer information and consumer information.[6] Each bank holding company must identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems. An assessment must be made of the (1) likelihood and potential damage of these threats, taking into consideration the sensitivity of the customer information, and (2) sufficiency of policies, procedures, customer information systems, and other arrangements that are in place to control risks.

Appropriate policies, procedures, training, and testing must be implemented to manage and control identified risks. Management must also report at least annually to the board of directors or an appropriate committee of the board. Management's reports should describe the overall status of the information security program and the bank holding company's compliance with the information security standards. The reports should discuss material matters related to the BHC's information security program, addressing issues such as risk assessment, risk-management and -control decisions, service-provider arrangements, results of testing, security breaches or violations and management's responses to them, and recommendations for changes in the information security program.

The information security standards outline specific information security measures that bank holding companies must consider in implementing an information security program. A bank holding company should adopt appropriate measures to manage and control identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of its activities. The measures that a bank holding company must consider and may adopt include access controls, access restrictions, encryption of electronic customer information, dual control procedures, segregation of duties, and employee background checks for employees who have responsibilities for or access to customer information. In addition, a bank holding company must have monitoring systems and response programs and measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures. Training and testing, are critical components to implement an effective information security program. Each bank holding company must regularly test the key controls, systems, and procedures. Tests should be conducted or reviewed by independent third parties or by staff who are independent of the individuals who develop or maintain the security program.

The Federal Reserve recognizes that banking organizations are highly sensitive to the importance of safeguarding customer information and the need to maintain effective information security programs. Existing examination and inspection procedures and supervisory processes already address information security. As a result, most banking organizations may not need to implement any new controls and procedures.

Examiners should assess compliance with the information security standards during each safety-and-soundness inspection, which may include targeted reviews of information technol-

public personal information, as defined in Regulation P, about a financial institution's customer that is maintained by or on behalf of the bank holding company.

6. A *customer* is defined in the same manner in Regulation P—a consumer who has established a continuing relationship with a bank holding company, under which the bank holding company provides one or more financial products or services to the consumer to be used primarily for personal, family, or household purposes. The definition of customer does not include a business, nor does it include a consumer who has not established an ongoing relationship with the bank holding company.

ogy. Ongoing compliance with the information security standards should be monitored as needed during the risk-focused inspection process. Material instances of noncompliance should be noted in the inspection report.

Bank holding companies are required to oversee their service-provider arrangements in order to (1) protect the security of customer information maintained or processed by their service providers; (2) ensure that their service providers properly dispose of customer and consumer information; and (3) whenever warranted, monitor their service providers to confirm that a provider has satisfied its contractual obligations.

A bank holding company must use appropriate due diligence in selecting its service providers. Bank holding companies should review a potential service provider's information security program or the measures the service provider will use to protect the bank holding company's customer information.[7] All contracts must require that the service provider implement appropriate measures designed to meet the objectives of the information security standards.

When indicated by the bank holding company's risk assessment, the performance of its service providers must be monitored to confirm that they have satisfied their obligations under the information security program. A bank holding company's methods for overseeing its service providers may differ depending on the type of services, the service provider, or the level of risk to the customer information. For example, if a service provider is subject to regulations or a code of conduct that imposes a duty to protect customer information consistent with the objectives of the information security standards, a bank holding company may consider that duty in exercising its due diligence and oversight of the service provider. If a service provider hires a subservicer (that is, subcontracts), the subservicer would not be considered a "service provider" under the guidelines.

2124.4.1.1 Disposal of Customer and Consumer Information

The information security standards address standards for the proper disposal of consumer information, pursuant to sections 621 and 628 of the Fair Credit Reporting Act (15 U.S.C. 1681s and 1681w). Under section 225.4 of Regulation Y, a BHC is required to properly dispose of consumer information in accordance with 16 C.F.R. 682. To address the risks associated with identity theft, a BHC and its nonbank subsidiaries and affiliates (a financial institution) is generally required to develop, implement, and maintain, as part of its existing information security program, appropriate measures to properly dispose of consumer information derived from consumer reports.

Consumer information is defined as any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report and that is maintained or otherwise possessed by or on behalf of the banking organization for a business purpose. Consumer information also means a compilation of such records.

The following are examples of consumer information:

1. a consumer report that a bank obtains
2. information from a consumer report that the bank obtains from its affiliate after the consumer has been given a notice and has elected not to opt out of that sharing
3. information from a consumer report that the bank obtains about an individual who applies for but does not receive a loan, including any loan sought by an individual for a business purpose
4. information from a consumer report that the bank obtains about an individual who guarantees a loan (including a loan to a business entity)
5. information from a consumer report that the bank obtains about an employee or prospective employee

Consumer information does not include any record that does not personally identify an individual, nor does it include the following:

1. aggregate information, such as the mean credit score, derived from a group of consumer reports
2. blind data, such as payment history on accounts that are not personally identifiable, that may be used for developing credit scoring models or for other purposes

7. A *service provider* is deemed to be a person or entity that maintains, processes, or is otherwise permitted access to customer information through its direct provision of services directly to the bank holding company.

2124.4.2 RESPONSE PROGRAMS FOR UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION AND CUSTOMER NOTICE

The information security standards list measures to be included in a bank holding company's information security program. These measures include ''response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.''[8] A response program is the principal means for a financial institution to protect against the unauthorized ''use'' of customer information that could lead to ''substantial harm or inconvenience'' for its customer. For example, customer notification is an important tool that enables a customer to take steps to prevent identity theft, such as by arranging to have a fraud alert placed in his or her credit file.

Prompt action by both the institution and the customer following any unauthorized access to customer information is crucial to preventing or limiting damages from identity theft. As a result, every financial institution should develop and implement a response program appropriate to its size and complexity and to the nature and scope of its activities. The program should be designed to address incidents of unauthorized access to customer information.

The Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice[9] (the guidance) interprets section 501(b) of the Gramm-Leach-Bliley Act (the GLB Act) and the information security standards.[10] The guidance describes the response programs, including customer notification procedures, that a financial institution should develop and implement to address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer.

When evaluating the adequacy of an institution's required information security program, examiners are to consider whether the institution has developed and implemented a response program equivalent to the guidance. At a minimum, an institution's response program should contain procedures for (1) assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused; (2) notifying its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of *sensitive* customer information, as defined later in the guidance; (3) immediately notifying law enforcement in situations involving federal criminal violations requiring immediate attention; (4) taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, such as by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and (5) notifying customers when warranted.

The guidance does not apply to a financial institution's foreign offices, branches, or affiliates. However, a financial institution subject to the information security standards is responsible for the security of its customer information, whether the information is maintained within or outside of the United States, such as by a service provider located outside of the United States.

The guidance also applies to customer information, meaning any record containing nonpublic personal information about a financial institution's customer, whether in paper, electronic, or other form, *that is maintained by or on behalf of the institution*.[11] (See the Board's privacy rule, Regulation P, at section 216.3(n)(2) (12 C.F.R. 216.3(n)(2).) Consequently, the guidance applies only to information that is within the control of the institution and its service providers. The guidance would not apply to information directly disclosed by a customer to a third party, for example, through a fraudulent web site.

The guidance also does not apply to information involving business or commercial accounts. Instead, the guidance applies to nonpublic personal information about a ''customer'' as that term is used in the information security standards, namely, a consumer who obtains a financial product or service from a financial institution to be used primarily for personal, family, or

8. See the information security standards, 12 CFR 225, appendix F, supplement A.

9. The guidance was jointly issued on March 23, 2005 (effective March 29, 2005), by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

10. See 12 C.F.R. 225, appendix F. The Interagency Guidelines Establishing Information Security Standards were formerly known as the Interagency Guidelines Establishing Standards for Safeguarding Customer Information.

11. See the information security standards, 12 C.F.R. 225, appendix F, section I.C.2.c.

household purposes, and who has a continuing relationship with the institution.[12]

2124.4.2.1 Response Programs

Financial institutions should take preventive measures to safeguard customer information against attempts to gain unauthorized access to the information. For example, financial institutions should place access controls on customer information systems and conduct background checks on employees who are authorized to access customer information.[13] However, every financial institution should also develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems[14] that occur nonetheless. A response program should be a key part of an institution's information security program. The program should be appropriate to the size and complexity of the institution and the nature and scope of its activities.

In addition, each institution should be able to address incidents of unauthorized access to customer information in customer information systems maintained by its domestic and foreign service providers. Therefore, consistent with the obligations in the information security standards that relate to these arrangements and with existing guidance on this topic issued by the agencies, an institution's contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to the financial institution's customer information. These actions include notifying the institution as soon as possible of any such incident, which enables the institution to expeditiously implement its response program.

2124.4.2.1.1 Components of a Response Program

At a minimum, an institution's response program should contain procedures for the following:

1. assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused
2. notifying its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of *sensitive* customer information, as defined below
3. consistent with the Suspicious Activity Report (SAR) regulations,[15] notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing
4. taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence
5. notifying customers when warranted

As noted above for the second component, a financial institution and a bank holding company are to notify its primary federal regulator of a security breach involving sensitive customer information, whether or not it notifies its customers. The banking organization experiencing such a breach should promptly notify its supervisory central point of contact at its Reserve Bank and provide information on the nature of the incident and on whether law enforcement authorities were notified or a SAR was or will be filed. When reporting security breaches involving sensitive customer information, the institution should provide the central point of contact with information on the steps taken to contain and control the incident, the

12. See the information security standards, 12 C.F.R. 225, appendix F, at section I.C.2.b. and the Board's Privacy Rule (Regulation P), section 216.3(h) (12 C.F.R. 216.3(h)).

13. Institutions should also conduct background checks on employees to ensure that they do not violate 12 U.S.C. 1829, which prohibits an institution from hiring an individual convicted of certain criminal offenses or who is subject to a prohibition order under 12 U.S.C. 1818(e)(6).

14. Under the information security standards, an institution's *customer information systems* consist of all the methods used to access, collect, store, use, transmit, protect, or dispose of customer information, including the systems maintained by its service providers. See the information security standards, 12 C.F.R. 225, appendix F, section I.C.2.d.

15. An institution's obligation to file a SAR is set out in the SAR regulations and supervisory guidance. See 12 C.F.R. 208.62 (state member banks); 12 C.F.R. 211.5(k) (Edge and agreement corporations); 12 C.F.R. 211.24(f) (uninsured state branches and agencies of foreign banks); and 12 C.F.R. 225.4(f) (bank holding companies and their nonbank subsidiaries). See also SR-01-11, "Identity Theft and Pretext Calling."

number of customers potentially affected, whether customer notification is warranted, and whether a service provider was involved. A banking organization should not delay providing prompt initial notification to its central point of contact. (See SR-05-23/CA-05-10.)

If an incident of unauthorized access to customer information involves customer information systems maintained by an institution's service providers, the financial institution is responsible for notifying its customers and regulator. However, an institution may authorize or contract with its service provider to notify the institution's customers or regulator on its behalf.

2124.4.2.2 Customer Notice

Financial institutions have an affirmative duty to protect their customers' information against unauthorized access or use. Notifying customers of a security incident involving the unauthorized access or use of the customer information, in accordance with the standard set forth below, is a key part of that duty.

Timely notification of customers is important to managing an institution's reputation risk. Effective notice also may reduce an institution's legal risk, assist in maintaining good customer relations, and enable the institution's customers to take steps to protect themselves against the consequences of identity theft. When customer notification is warranted, an institution may not forgo notifying its customers of an incident because the institution believes that it may be potentially embarrassed or inconvenienced by doing so.

2124.4.2.2.1 Standard for Providing Notice

When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible.

Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation.

2124.4.2.2.2 Sensitive Customer Information

Under the information security standards, an institution must protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. Substantial harm or inconvenience is most likely to result from improper access to *sensitive customer information* because this type of information is most likely to be misused, as in the commission of identity theft.

For purposes of the guidance, *sensitive customer information* means a customer's name, address, or telephone number, in conjunction with the customer's Social Security number, driver's license number, account number, credit or debit card number, or with a personal identification number or password that would permit access to the customer's account. *Sensitive customer information* also includes any combination of components of customer information that would allow someone to log on to or access the customer's account, such as a user name and password or a password and an account number.

2124.4.2.2.3 Affected Customers

If a financial institution, on the basis of its investigation, can determine from its logs or other data precisely which customers' information has been improperly accessed, it may limit notification to those customers for whom the institution determines that misuse of their information has occurred or is reasonably possible. However, there may be situations in which an institution determines that a group of files has been accessed improperly but is unable to identify which specific customers' information has been accessed. If the circumstances of the unauthorized access lead the institution to determine that misuse of the information is reasonably possible, it should notify all customers in the group.

2124.4.2.2.4 Content of Customer Notice

Customer notice should be given in a clear and conspicuous manner. The notice should describe the incident in general terms and the type of customer information that was the subject of unauthorized access or use. The notice should also generally describe what the institution has done to protect the customers' information from further unauthorized access, and include a telephone number that customers can call for further information and assistance.[16] The notice should remind customers of the need to remain vigilant over the next 12 to 24 months, and to promptly report incidents of suspected identity theft to the institution. The notice should include the following additional items, when appropriate:

1. a recommendation that the customer review account statements and immediately report any suspicious activity to the institution
2. a description of fraud alerts and an explanation of how the customer may place a fraud alert in his or her consumer reports to put the customer's creditors on notice that the customer may be a victim of fraud
3. a recommendation that the customer periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted
4. an explanation of how the customer may obtain a credit report free of charge
5. information about the availability of the Federal Trade Commission (FTC) online guidance regarding steps consumers can take to protect themselves against identity theft (The notice should encourage the customer to report any incidents of identity theft to the FTC and should provide the FTC's web site address and toll-free telephone number that customers may use to obtain the identity theft guidance and to report suspected incidents of identity theft.)[17]

Financial institutions are encouraged to notify the nationwide consumer reporting agencies before sending notices to a large number of customers when those notices include contact information for the reporting agencies.

2124.4.2.2.5 Delivery of Customer Notice

Customer notice should be delivered in any manner designed to ensure that a customer can reasonably be expected to receive it. For example, the institution may choose to contact all affected customers by telephone, by mail, or by electronic mail in the case of customers for whom it has a valid e-mail address and who have agreed to receive communications electronically.

2124.4.3 Inspection Objective

1. To review and assess the bank holding company's compliance with the Interagency Guidelines Establishing Information Security Standards, which include standards for safeguarding customer information (the examiners should thus review the BHC's information security program, including its response program for unauthorized access to customer information and customer notice and its guidelines on the proper disposal of customer information and consumer information) and all other applicable laws, rules, and regulations.

2124.4.4 Inspection Procedures

1. Referencing the ''Establishment of Information Security Standards'' section of the internal control questionnaire in section 4060.4 of the System's *Commercial Bank Examination Manual,* assess the BHC's compliance with the Interagency Guidelines Establishing Information Security Standards including its standards for safeguarding customer information.
2. Conduct a review that is a sufficient basis for evaluating the BHC's overall information security program and its compliance with the information security standards.

16. The institution should, therefore, ensure that it has reasonable policies and procedures in place, including trained personnel, to respond appropriately to customer inquiries and requests for assistance.

17. The FTC web site for the ID theft brochure and the FTC hotline phone number are www.ftc.gov/bcp/consumer.shtm and 1-877-IDTHEFT. The institution may also refer customers to any materials developed pursuant to section 151(b) of the FACT Act (educational materials developed by the FTC to teach the public how to prevent identity theft).

2124.4.5 APPENDIX A—INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS

Sections II and III of the information security standards are provided below. For more information, see the Interagency Guidelines Establishing Information Security Standards in Regulation Y, section 225, appendix F (12 C.F.R. 225, appendix F). The guidelines were previously titled Interagency Guidelines Establishing Standards for Safeguarding Customer Information. The information security standards were amended, effective July 1, 2005, to implement section 216 of the Fair and Accurate Credit Transactions Act of 2003 (the FACT Act). To address the risks associated with identity theft, the amendments generally require financial institutions to develop, implement, and maintain, as part of their existing information security program, appropriate measures to properly dispose of consumer information derived from consumer reports. The term *consumer information* is defined in the revised rule.

II. Standards for Safeguarding Customer Information

A. Information Security Program

Each bank holding company is to implement a comprehensive, written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank holding company and the nature and scope of its activities. While all parts of the bank holding company are not required to implement a uniform set of policies, all elements of the information security program are to be coordinated. A bank holding company is also to ensure that each of its subsidiaries is subject to a comprehensive information security program. The bank holding company may fulfill this requirement either by including a subsidiary within the scope of the bank holding company's comprehensive information security program or by causing the subsidiary to implement a separate comprehensive information security program in accordance with the standards and procedures in sections II and III that apply to bank holding companies.

B. Objectives

A bank holding company's information security program shall be designed to—

1. ensure the security and confidentiality of customer information;
2. protect against any anticipated threats or hazards to the security or integrity of such information;
3. protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer; and
4. ensure the proper disposal of customer information and consumer information.

III. Development and Implementation Of Information Security Program

A. Involve the Board of Directors

The board of directors or an appropriate committee of the board of each bank holding company is to—

1. approve the bank holding company's written information security program; and
2. oversee the development, implementation, and maintenance of the bank holding company's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

B. Assess Risk

Each bank holding company is to—

1. identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;
2. assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information;
3. assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks; and
4. ensure the proper disposal of customer information and consumer information.

C. Manage and Control Risk

Each bank holding company is to—

1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank holding company's activities. Each bank holding company must consider whether the following security measures are appropriate for the bank holding company and, if so, adopt those measures the bank holding company concludes are appropriate:
   a. access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means
   b. access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;
   c. encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access
   d. procedures designed to ensure that customer information system modifications are consistent with the bank holding company's information security program
   e. dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer Information
   f. monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems
   g. response programs that specify actions to be taken when the bank holding company suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies
   h. measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures
2. Train staff to implement the bank holding company's information security program.
3. Regularly test the key controls, systems, and procedures of the information security program. The frequency and nature of such tests should be determined by the bank holding company's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.
4. Develop, implement, and maintain, as part of its information security program, appropriate measures to properly dispose of customer information and consumer information in accordance with each of the requirements in this section III.

D. Oversee Service-Provider Arrangements

Each bank holding company is to—

1. exercise appropriate due diligence in selecting its service providers;
2. require its service providers by contract to implement appropriate measures designed to meet the objectives of the information security standards; and
3. where indicated by the bank holding company's risk assessment, monitor its service providers to confirm that they have satisfied their obligations with regard to the requirements for overseeing provider arrangements. As part of this monitoring, a bank holding company should review audits, summaries of test results, or other equivalent evaluations of its service providers.

E. Adjust the Program

Each bank holding company is to monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the bank holding company's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.

F. Report to the Board

Each bank holding company is to report to its board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the bank holding company's compliance with the information security standards. The reports should discuss material matters related to its program, addressing issues such as risk assessment; risk management and control decisions; service-provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for changes in the information security program.

G. Implement the Standards

For effective dates, see 12 C.F.R. 225, appendix F, section III.G.

2124.5.1 IDENTITY THEFT RED FLAGS PREVENTION PROGRAM

The federal financial institution regulatory agencies[1] and the Federal Trade Commission (FTC) have issued joint regulations and guidelines on the *detection*, *prevention*, and *mitigation* of identity theft in connection with opening of certain accounts or maintaining certain existing accounts in response to the Fair and Accurate Credit Transactions Act of 2003 (The FACT Act).[2] Under the FACT Act, bank holding companies (BHCs) and their nonbank subsidiaries are subject to the FTC's regulations.[3] These regulations require financial institutions[4] or creditors[5] that offer or maintain one or more "covered accounts" to develop and implement a written Identity Theft Prevention Program (Program). A Program is to be designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program must be tailored to the entity's size, complexity, and the nature and scope of its operations and activities. The regulations also require (debit and credit) card issuers to validate notifications of changes of address under certain circumstances.

The joint final rules and guidelines were effective on January 1, 2008. The mandatory compliance date for the rules was November 1, 2008.[6] (See section 681 of the FTC's Red Flags Rule (16 CFR 681) and 72 *Fed. Reg.* 63718-63775, November 9, 2007.)

This section describes the provisions of the Red Flags Rule and its guidelines (appendix A) to be used when examining a BHC and its nonbank subsidiaries over which the Federal Reserve has supervisory authority (collectively referred to as "BHC"). (See SR-08-7/CA-08-10 and its interagency attachments.)

2124.5.1.1 Risk Assessment

Prior to the development of the Program, a financial institution or creditor must initially and then periodically conduct a risk assessment to determine whether it offers or maintains covered accounts. It must take into consideration (1) the methods it provides to open its accounts, (2) the methods it provides to access accounts, and (3) its previous experiences with identity theft. If the financial institution or creditor has covered accounts, it must evaluate its potential vulnerability to identity theft. The institution should also consider whether a reasonably foreseeable risk of identity theft may exist in connection with the accounts it offers or maintains and those that may be opened or accessed remotely, through methods that do not require face-to-face contact, such as through the Internet or telephone. Financial institutions or creditors that offer or maintain business accounts that have been the target of identity theft should factor those experiences with identity theft into their determination.

If the financial institution or creditor determines that it has covered accounts, the risk assessment will enable it to identify which of its accounts the Program must address. If a financial institution or creditor initially determines that it does *not* have covered accounts, it must periodically reassess whether it must develop and implement a Program in light of changes in the accounts that it offers or maintains.

1. The Board of Governors of the Federal Reserve System (FRB), the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision (OTS), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA).

2. Section 111 of the FACT Act defines "identity theft" as "a fraud committed or attempted using the identifying information of another person."

3. The FACT Act gives the Board the authority to write rules for state member banks but not BHCs. Nonetheless, the Board retains its supervisory and enforcement authority over BHCs, pursuant to section 1818 of the Federal Deposit Insurance Act. The Board and FTC Red Flags Rules are substantially the same.

4. For purposes of the rule, the term "financial institution" means a "State or National bank, a State or Federal savings and loan association, a mutual savings bank . . . or any other person that, directly or indirectly, holds a transaction account . . . belonging to a consumer."

5. Under section 111 of the FACT Act, the term "creditor" means any person (a natural person, a corporation, government or governmental subdivision, trust, estate, partnership, cooperative, or association) who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee or original creditor who participates in the decision to extend, renew, or continue credit.

6. The FTC subsequently granted a six-month delay of enforcement of its Red Flags Rule until May 1, 2009. (See www2.ftc.gov/opa/2008/10/redflags.shtm.) This delay in enforcement is limited to the Identity Theft Red Flags Rule (16 CFR 681.1), and does not extend to the rule regarding changes of address applicable to card issuers (16 C.F.R. 681.2).

2124.5.1.2 Elements of the Program

The elements of the actual Program will vary depending on the size and complexity of the financial institution or creditor. A financial institution or creditor that determines that it is required to establish and maintain an Identity Theft Prevention Program must (1) identify relevant Red Flags for its covered accounts, (2) detect the Red Flags that have been incorporated into its Program, and (3) respond appropriately to the detected Red Flags. The Red Flags are patterns, practices, or specific activities that indicate the possible existence of identity theft or the potential to lead to identity theft. A financial institution or creditor must ensure (1) that its Program is updated periodically to address the changing risks associated with its customers and their accounts and (2) the safety and soundness of the financial institution or creditor from identity theft.

2124.5.1.3 Guidelines

Each financial institution or creditor that is required to implement a written Program must consider the Guidelines for Identity Theft Detection, Prevention, and Mitigation (16 C.F.R. 681, appendix A of the rule) (the Guidelines) and include those guidelines that are appropriate in its Program. Section I of the Guidelines, ''The Program,'' discusses a Program's design that may include, as appropriate, existing policies, procedures, and arrangements that control foreseeable risks to the institution's customers or to the safety and soundness of the financial institution or creditor from identity theft.

2124.5.1.3.1 Identification of Red Flags

A financial institution or creditor should incorporate relevant Red Flags into the Program from sources such as (1) incidents of identity theft that it has experienced, (2) methods of identity theft that have been identified as reflecting changes in identity theft risks, and (3) applicable supervisory guidance.

2124.5.1.3.2 Categories of Red Flags

Section II of the Guidelines, ''Categories of Red Flags,'' provides some guidance in identifying relevant Red Flags.[7] A financial institution or creditor should include, as appropriate,

1. alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
2. the presentation of suspicious documents;
3. the presentation of suspicious personal identifying information, such as a suspicious address change;
4. the unusual use of, or other suspicious activity related to, a covered account; and
5. notices received from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

The above categories do not represent a comprehensive list of all types of Red Flags that may indicate the possibility of identity theft. Institutions must also consider specific business lines and any previous exposures to identity theft. No specific Red Flag is mandatory for all financial institutions or creditors. Rather, the Program should follow the risk-based, nonprescriptive approach regarding the identification of Red Flags.

2124.5.1.3.3 Detect the Program's Red Flags

In accordance with Section III of the Guidelines, each financial institution or creditor's Program should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts. A financial institution or creditor is required to detect, prevent, and mitigate identity theft in connection with such accounts. The policies and procedures regarding opening a covered account subject to the Program should explain how an institution could identify information about, and verify the identity of, a person opening an account.[8] In the case of existing covered accounts, institutions could authenticate customers, monitor transactions, and verify the validity of change of address requests.

7. Examples of Red Flags from each of these categories are appended as supplement A to appendix A.
8. See 31 U.S.C. 5318(l) and 31 C.F.R. 103.121.

2124.5.1.3.4 Respond Appropriately to any Detected Red Flags

A financial institution or creditor should consider precursors to identity theft to stop identity theft before it occurs. Section IV of the Guidelines, ''Prevention and Mitigation,'' states that an institution's procedures should provide for appropriate responses to Red Flags that it has detected that are commensurate with the degree of risk posed. When determining an appropriate response, the institution should consider aggravating factors that may heighten its risk of identity theft. Such factors may include (1) a data security incident that results in unauthorized disclosures of nonpublic personal information, (2) records the institution holds or that are held by another creditor or third party, or (3) notice that the institution's customer has provided information related to its covered account to someone fraudulently claiming to represent the institution or to a fraudulent website. Appropriate responses may include the following: (1) monitoring a covered account for evidence of identity theft; (2) contacting the customer; (3) changing any passwords, security codes, or other security devices that permit access to a secured account; (4) reopening a covered account with a new account number; (5) not opening a new covered account; (6) closing an existing covered account; (7) not attempting to collect on a covered account or not selling a covered account to a debt collector; (8) notifying law enforcement; or (9) determining that no response is warranted under the particular circumstances.

2124.5.1.3.5 Periodically Updating the Program's Relevant Red Flags

Section V of the Guidelines, ''Updating the Program,'' states that a financial institution or creditor should periodically update its Program (including its relevant Red Flags) to reflect any changes in risks to its customers or to the safety and soundness of the institution from identity theft, based on (but not limited to) factors such as

1. the experiences of the institution with identity theft,
2. changes in methods of identity theft,
3. changes in methods to detect, prevent, and mitigate identity theft,
4. changes in the types of accounts that the institution offers or maintains, and
5. changes in the institution's structure, including its mergers, acquisitions, joint ventures, and any business arrangements, such as alliances and service provider arrangements.

2124.5.1.4 Administration of Program

A financial institution or creditor that is required to implement a Program must provide for the continued oversight and administration of its Program. The following are the steps that are needed in the administration of a Red Flags Program:

1. *Obtain approval from either the institution's board of directors or any appropriate committee of the board of directors of the initial written Program;*
2. *Involve either the board of directors, a designated committee of the board of directors, or a designated senior-management-level employee in the oversight, development, implementation, and administration of the Program.*[9] This includes
   - assigning specific responsibility for the Program's implementation,
   - reviewing reports prepared by staff regarding the institution's compliance (the reports should be prepared at least annually), and
   - reviewing material changes to the Program as necessary to address changing identity theft risks.
3. *Train staff.* The financial institution or creditor must train relevant staff to effectively implement and monitor the Program. Training should be provided as changes are made to the financial institution or creditor's Program based on its periodic risk assessment.
4. *Exercise appropriate and effective oversight of service provider arrangements.* Section VI of the Guidelines, ''Methods for Administering the Program,'' indicates a financial institution or creditor is ultimately responsible for complying with the rules and guidelines for outsourcing an activity to a third-party

9. BHC subsidiaries can use the security program developed at the holding company level. However, if subsidiary institutions choose to use a security program developed at the holding company level, the board of directors or an appropriate committee at each subsidiary institution must conduct an independent review to ensure that the program is suitable and complies with the requirements prescribed by its primary regulator.

service provider. Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts, the institution should ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. With regard to the institution's oversight of its Program, periodic reports from service providers are to be issued on the Program's development, implementation, and administration.

2124.5.2 INSPECTION OBJECTIVES

1. To determine if the BHC has developed, implemented, and maintained a written Program for new and existing accounts that are covered by the FACT Act and the Federal Trade Commission's rules on Fair Credit Reporting, section 681, Subpart A—Identity Theft Red Flags (16 C.F.R. 681, subpart A), which implements provisions of the FACT Act.
2. To make a determination of whether the Program is
   a. designed to detect, prevent, and mitigate identity theft in connection with the opening of a new, or an existing, covered account and if the Program includes the detection of relevant ''Red Flags'' and
   b. appropriate to the size and complexity of the ''financial institution'' or ''creditor'' and the nature and scope of its activities.
3. To ascertain whether the BHC assesses the validity of change of address notifications that it receives for the credit and debit cards that it has issued to customers.

2124.5.3 INSPECTION PROCEDURES

1. Verify that the BHC has determined initially, and periodically thereafter, whether it offers or maintains accounts covered by the FACT Act and section 681, Subpart A—Identity Theft Red Flags (16 C.F.R. 681, subpart A).
2. Determine if the BHC has adequately developed and maintains a written Program that is designed to detect, prevent, and monitor transactions to mitigate identity theft in connection with the opening of certain new and existing accounts covered by the FACT Act.
3. Evaluate whether the Program includes reasonable policies and procedures to
   a. identify and detect relevant Red Flags for the BHC's covered accounts and whether it incorporated those Red Flags into its Program,
   b. respond appropriately to any detected Red Flags to prevent and mitigate identity theft, and
   c. ensure that the Program is updated periodically to reflect changes in identity theft risks to the customers and the safety and soundness of the institution.
4. If a required Program has been established by the BHC, ascertain if it has provided for the Program's continued administration, including
   a. involving the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the continued oversight, development, implementation, and administration of the Program;
   b. training staff, as necessary, to effectively implement the Program; and
   c. appropriate and effective oversight of service provider arrangements.
5. If the BHC has established and maintains a required Program that applies to its covered accounts, determine if the Program includes the relevant and appropriate guidelines within the rule's appendix A (16 C.F.R. 681, appendix A).

Banking organizations should be attentive to the possible adverse consequences (including financial loss) of decisions based on models that are incorrect or misused and should address those consequences through active model risk management. The key aspects of an effective model risk-management framework are described in more detail below, including robust model development, implementation, and use; effective validation; and sound governance, policies, and controls. (See SR-11-7.)

2126.0.1 INTRODUCTION—PART I

Banks rely heavily on quantitative analysis and models in most aspects of financial decision making.[1] They routinely use models for a broad range of activities, including underwriting credits; valuing exposures, instruments, and positions; measuring risk; managing and safeguarding client assets; determining capital and reserve adequacy; and many other activities. In recent years, banks have applied models to more complex products and with more ambitious scope, such as enterprise-wide risk measurement, while the markets in which they are used have also broadened and changed. Changes in regulation have spurred some of the recent developments, particularly the U.S. regulatory capital rules for market, credit, and operational risk based on the framework developed by the Basel Committee on Banking Supervision. Even apart from these regulatory considerations, however, banks have been increasing the use of data-driven, quantitative decision making tools for a number of years.

The expanding use of models in all aspects of banking reflects the extent to which models can improve business decisions, but models also come with costs. There is the direct cost of devoting resources to develop and implement models properly. There are also the potential indirect costs of relying on models, such as the possible adverse consequences (including financial loss) of decisions based on models that are incorrect or misused. Those consequences should be addressed by active management of model risk.

This guidance describes the key aspects of effective model risk management. Part II explains the purpose and scope of the guidance, and part III gives an overview of model risk management. Part IV discusses robust model development, implementation, and use. Part V describes the components of an effective validation framework. Part VI explains the salient features of sound governance, policies, and controls over model development, implementation, use, and validation. Part VII concludes.

2126.0.2 PURPOSE AND SCOPE—PART II

The purpose of this section is to provide comprehensive guidance for banks on effective model risk management. Rigorous model validation plays a critical role in model risk management; however, sound development, implementation, and use of models are also vital elements. Furthermore, model risk management encompasses governance and control mechanisms such as board and senior management oversight, policies and procedures, controls and compliance, and an appropriate incentive and organizational structure.

Previous guidance and other publications issued by the Office of the Comptroller of the Currency (OCC) and the Federal Reserve on the use of models pay particular attention to model validation.[2] Based on supervisory and industry experience over the past several years, this document expands on existing guidance—most importantly by broadening the scope to include all aspects of model risk management. Many banks may already have in place a large portion of these practices, but all banks should ensure that internal policies and procedures are consis-

1. Unless otherwise indicated, *banks* refers to national banks and all other institutions for which the Office of the Comptroller of the Currency is the primary supervisor, and to bank holding companies, state member banks, and all other institutions for which the Federal Reserve Board is the primary supervisor.

2. For instance, the OCC provided guidance on model risk, focusing on model validation, in OCC 2000-16 (May 30, 2000), other bulletins, and certain subject matter booklets of the *Comptroller's Handbook.* The Federal Reserve issued SR-09-01, "Application of the Market Risk Rule in Bank Holding Companies and State Member Banks," which highlights various concepts pertinent to model risk management, including standards for validation and review, model validation documentation, and back-testing. The Federal Reserve's *Trading and Capital-Markets Activities Manual* also discusses validation and model risk management. In addition, the advanced-approaches risk-based capital rules (12 CFR 3, Appendix C; 12 CFR 208, Appendix F; and 12 CFR 225, Appendix G) contain explicit validation requirements for subject banking organizations.

tent with the risk-management principles and supervisory expectations contained in this guidance. Details may vary from bank to bank, as practical application of this guidance should be customized to be commensurate with a bank's risk exposures, its business activities, and the complexity and extent of its model use. For example, steps taken to apply this guidance at a community bank using relatively few models of only moderate complexity might be significantly less involved than those at a larger bank where use of models is more extensive or complex.

2126.0.3 OVERVIEW OF MODEL RISK MANAGEMENT—PART III

For the purposes of this section, the term *model* refers to a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates. A *model* consists of three components: an information input component, which delivers assumptions and data to the model; a processing component, which transforms inputs into estimates; and a reporting component, which translates the estimates into useful business information. Models meeting this definition might be used for analyzing business strategies; informing business decisions; identifying and measuring risks; valuing exposures, instruments, or positions; conducting stress testing; assessing adequacy of capital; managing client assets; measuring compliance with internal limits; maintaining the formal control apparatus of the bank; meeting financial or regulatory reporting requirements; and issuing public disclosures. The definition of *model* also covers quantitative approaches whose inputs are partially or wholly qualitative or based on expert judgment, provided that the output is quantitative in nature.[3]

Models are simplified representations of real-world relationships among observed characteristics, values, and events. Simplification is inevitable, due to the inherent complexity of those relationships, but also intentional, to focus attention on particular aspects considered to be most important for a given model application. Model quality can be measured in many ways: precision, accuracy, discriminatory power, robustness, stability, and reliability, to name a few. Models are never perfect, and the appropriate metrics of quality, and the effort that should be put into improving quality, depend on the situation. For example, precision and accuracy are relevant for models that forecast future values, while discriminatory power applies to models that rank order risks. In all situations, it is important to understand a model's capabilities and limitations given its simplifications and assumptions.

The use of models invariably presents model risk, which is the potential for adverse consequences from decisions based on incorrect or misused model outputs and reports. Model risk can lead to financial loss, poor business and strategic decision making, or damage to a bank's reputation. Model risk occurs primarily for two reasons:

- The model may have fundamental errors and may produce inaccurate outputs when viewed against the design objective and intended business uses. The mathematical calculation and quantification exercise underlying any model generally involves application of theory, choice of sample design and numerical routines, selection of inputs and estimation, and implementation in information systems. Errors can occur at any point from design through implementation. In addition, shortcuts, simplifications, or approximations used to manage complicated problems could compromise the integrity and reliability of outputs from those calculations. Finally, the quality of model outputs depends on the quality of input data and assumptions, and errors in inputs or incorrect assumptions will lead to inaccurate outputs.
- The model may be used incorrectly or inappropriately. Even a fundamentally sound model producing accurate outputs consistent with the design objective of the model may exhibit high model risk if it is misapplied or misused. Models by their nature are simplifications of reality, and real-world events may prove those simplifications inappropriate. This is even more of a concern if a model is used outside the environment for which it was designed. Banks may do this intentionally as they apply existing models to new products or markets, or inadvertently as market conditions or customer behavior changes. Decision makers need to understand the limitations of a model to avoid using it in ways that are not consistent with the original intent. Limitations

3. While outside the scope of this guidance, more qualitative approaches used by banking organizations—i.e., those *not* defined as models according to this guidance—should also be subject to a rigorous control process.

come in part from weaknesses in the model due to its various shortcomings, approximations, and uncertainties. Limitations are also a consequence of assumptions underlying a model that may restrict the scope to a limited set of specific circumstances and situations.

Model risk should be managed like other types of risk. Banks should identify the sources of risk and assess the magnitude. Model risk increases with greater model complexity, higher uncertainty about inputs and assumptions, broader use, and larger potential impact. Banks should consider risk from individual models and in the aggregate. Aggregate model risk is affected by interaction and dependencies among models; reliance on common assumptions, data, or methodologies; and any other factors that could adversely affect several models and their outputs at the same time. With an understanding of the source and magnitude of model risk in place, the next step is to manage it properly.

A guiding principle for managing model risk is ''effective challenge'' of models, that is, critical analysis by objective, informed parties who can identify model limitations and assumptions and produce appropriate changes. Effective challenge depends on a combination of incentives, competence, and influence. Incentives to provide effective challenge to models are stronger when there is greater separation of that challenge from the model development process and when challenge is supported by well-designed compensation practices and corporate culture. Competence is a key to effectiveness since technical knowledge and modeling skills are necessary to conduct appropriate analysis and critique. Finally, challenge may fail to be effective without the influence to ensure that actions are taken to address model issues. Such influence comes from a combination of explicit authority, stature within the organization, and commitment and support from higher levels of management.

Even with skilled modeling and robust validation, model risk cannot be eliminated, so other tools should be used to manage model risk effectively. Among these are establishing limits on model use, monitoring model performance, adjusting or revising models over time, and supplementing model results with other analysis and information. Informed conservatism, in either the inputs or the design of a model or through explicit adjustments to outputs, can be an effective tool, though not an excuse to avoid improving models.

As is generally the case with other risks, materiality is an important consideration in model risk management. If at some banks the use of models is less pervasive and has less impact on their financial condition, then those banks may not need as complex an approach to model risk management in order to meet supervisory expectations. However, where models and model output have a material impact on business decisions, including decisions related to risk management and capital and liquidity planning, and where model failure would have a particularly harmful impact on a bank's financial condition, a bank's model risk-management framework should be more extensive and rigorous.

Model risk management begins with robust model development, implementation, and use. Another essential element is a sound model validation process. A third element is governance, which sets an effective framework with defined roles and responsibilities for clear communication of model limitations and assumptions, as well as the authority to restrict model usage. Each of these elements is discussed in the following sections.

2126.0.4 MODEL DEVELOPMENT, IMPLEMENTATION, AND USE—PART IV

Model risk management should include disciplined and knowledgeable development and implementation processes that are consistent with the situation and goals of the model user and with bank policy. Model development is not a straightforward or routine technical process. The experience and judgment of developers, as much as their technical knowledge, greatly influence the appropriate selection of inputs and processing components. The training and experience of developers exercising such judgment affects the extent of model risk. Moreover, the modeling exercise is often a multidisciplinary activity drawing on economics, finance, statistics, mathematics, and other fields. Models are employed in real-world markets and events and, therefore, should be tailored for specific applications and informed by business uses. In addition, a considerable amount of subjective judgment is exercised at various stages of model development, implementation, use, and validation. It is important for decision makers to recognize that this subjectivity elevates the importance of sound

and comprehensive model risk-management processes.[4]

2126.0.4.1 Model Development and Implementation

An effective development process begins with a clear statement of purpose to ensure that model development is aligned with the intended use. The design, theory, and logic underlying the model should be well documented and generally supported by published research and sound industry practice. The model methodologies and processing components that implement the theory, including the mathematical specification and the numerical techniques and approximations, should be explained in detail with particular attention to merits and limitations. Developers should ensure that the components work as intended, are appropriate for the intended business purpose, and are conceptually sound and mathematically and statistically correct. Comparison with alternative theories and approaches is a fundamental component of a sound modeling process.

The data and other information used to develop a model are of critical importance; there should be rigorous assessment of data quality and relevance, and appropriate documentation. Developers should be able to demonstrate that such data and information are suitable for the model and that they are consistent with the theory behind the approach and with the chosen methodology. If data proxies are used, they should be carefully identified, justified, and documented. If data and information are not representative of the bank's portfolio or other characteristics, or if assumptions are made to adjust the data and information, these factors should be properly tracked and analyzed so that users are aware of potential limitations. This is particularly important for external data and information (from a vendor or outside party), especially as they relate to new products, instruments, or activities.

An integral part of model development is testing, in which the various components of a model and its overall functioning are evaluated to determine whether the model is performing as intended. Model testing includes checking the model's accuracy, demonstrating that the model is robust and stable, assessing potential limitations, and evaluating the model's behavior over a range of input values. It should also assess the impact of assumptions and identify situations where the model performs poorly or becomes unreliable. Testing should be applied to actual circumstances under a variety of market conditions, including scenarios that are outside the range of ordinary expectations, and should encompass the variety of products or applications for which the model is intended. Extreme values for inputs should be evaluated to identify any boundaries of model effectiveness. The impact of model results on other models that rely on those results as inputs should also be evaluated. Included in testing activities should be the purpose, design, and execution of test plans, summary results with commentary and evaluation, and detailed analysis of informative samples. Testing activities should be appropriately documented.

The nature of testing and analysis will depend on the type of model and will be judged by different criteria depending on the context. For example, the appropriate statistical tests depend on specific distributional assumptions and the purpose of the model. Furthermore, in many cases statistical tests cannot unambiguously reject false hypotheses or accept true ones based on sample information. Different tests have different strengths and weaknesses under different conditions. Any single test is rarely sufficient, so banks should apply a variety of tests to develop a sound model.

Banks should ensure that the development of the more judgmental and qualitative aspects of their models is also sound. In some cases, banks may take statistical output from a model and modify it with judgmental or qualitative adjustments as part of model development. While such practices may be appropriate, banks should ensure that any such adjustments made as part of the development process are conducted in an appropriate and systematic manner and are well documented.

Models typically are embedded in larger information systems that manage the flow of data from various sources into the model and handle the aggregation and reporting of model outcomes. Model calculations should be properly coordinated with the capabilities and requirements of information systems. Sound model risk management depends on substantial investment in supporting systems to ensure data

4. Smaller banks that rely on vendor models may be able to satisfy the standards in this guidance without an in-house staff of technical, quantitative model developers. However, even if a bank relies on vendors for basic model development, the bank should still choose the particular models and variables that are appropriate to its size, scale, and lines of business and ensure the models are appropriate for the intended use.

and reporting integrity, together with controls and testing to ensure proper implementation of models, effective systems integration, and appropriate use.

2126.0.4.2 Model Use

Model use provides additional opportunity to test whether a model is functioning effectively and to assess its performance over time as conditions and model applications change. It can serve as a source of productive feedback and insights from a knowledgeable internal constituency with strong interest in having models that function well and reflect economic and business realities. Model users can provide valuable business insight during the development process. In addition, business managers affected by model outcomes may question the methods or assumptions underlying the models, particularly if the managers are significantly affected by, and do not agree with, the outcome. Such questioning can be healthy if it is constructive and causes model developers to explain and justify the assumptions and design of the models.

However, challenge from model users may be weak if the model does not materially affect their results, if the resulting changes in models are perceived to have adverse effects on the business line, or if change in general is regarded as expensive or difficult. User challenges also tend not to be comprehensive because they focus on aspects of models that have the most direct impact on the user's measured business performance or compensation, and thus may ignore other elements and applications of the models. Finally, such challenges tend to be asymmetric because users are less likely to challenge an outcome that results in an advantage for them. Indeed, users may incorrectly believe that model risk is low simply because outcomes from model-based decisions appear favorable to the institution. Thus, the nature and motivation behind model users' input should be evaluated carefully, and banks should also solicit constructive suggestions and criticism from sources independent of the line of business using the model.

Reports used for business decision making play a critical role in model risk management. Such reports should be clear and comprehensible and take into account the fact that decision makers and modelers often come from quite different backgrounds and may interpret the contents in different ways. Reports that provide a range of estimates for different input-value scenarios and assumption values can give decision makers important indications of the model's accuracy, robustness, and stability as well as information on model limitations.

An understanding of model uncertainty and inaccuracy and a demonstration that the bank is accounting for them appropriately are important outcomes of effective model development, implementation, and use. Because they are by definition imperfect representations of reality, all models have some degree of uncertainty and inaccuracy. These can sometimes be quantified, for example, by an assessment of the potential impact of factors that are unobservable or not fully incorporated in the model, or by the confidence interval around a statistical model's point estimate. Indeed, using a range of outputs, rather than a simple point estimate, can be a useful way to signal model uncertainty and avoid spurious precision. At other times, only a qualitative assessment of model uncertainty and inaccuracy is possible. In either case, it can be prudent for banks to account for model uncertainty by explicitly adjusting model inputs or calculations to produce more severe or adverse model output in the interest of conservatism. Accounting for model uncertainty can also include judgmental conservative adjustments to model output, placing less emphasis on that model's output, or ensuring that the model is only used when supplemented by other models or approaches.[5]

While conservative use of models is prudent in general, banks should be careful in applying conservatism broadly or claiming to make conservative adjustments or add-ons to address model risk, because the impact of such conservatism in complex models may not be obvious or intuitive. Model aspects that appear conservative in one model may not be truly conservative compared with alternative methods. For example, simply picking an extreme point on a given modeled distribution may not be conservative if the distribution was misestimated or misspecified in the first place. Furthermore, initially conservative assumptions may not remain conservative over time. Therefore, banks should justify and substantiate claims that model outputs are conservative with a definition and measurement of that conservatism that is communicated to model users. In some cases, sensitivity analysis or other types of stress testing can be used to

5. To the extent that models are used to generate amounts included in public financial statements, any adjustments for model uncertainty must comply with generally accepted accounting principles.

demonstrate that a model is indeed conservative. Another way in which banks may choose to be conservative is to hold an additional cushion of capital to protect against potential losses associated with model risk. However, conservatism can become an impediment to proper model development and application if it is seen as a solution that dissuades the bank from making the effort to improve the model; in addition, excessive conservatism can lead model users to discount the model outputs.

As previously explained, robust model development, implementation, and use is important to model risk management. But it is not enough for model developers and users to understand and accept the model. Because model risk is ultimately borne by the bank as a whole, the bank should objectively assess model risk and the associated costs and benefits using a sound model-validation process.

2126.0.5 MODEL VALIDATION—PART V

Model validation is the set of processes and activities intended to verify that models are performing as expected, in line with their design objectives and business uses. Effective validation helps ensure that models are sound. It also identifies potential limitations and assumptions and assesses their possible impact. As with other aspects of effective challenge, model validation should be performed by staff with appropriate incentives, competence, and influence.

All model components, including input, processing, and reporting, should be subject to validation; this applies equally to models developed in-house and to those purchased from, or developed by, vendors or consultants. The rigor and sophistication of validation should be commensurate with the bank's overall use of models, the complexity and materiality of its models, and the size and complexity of the bank's operations.

Validation involves a degree of independence from model development and use. Generally, validation should be done by people who are not responsible for development or use and do not have a stake in whether a model is determined to be valid. Independence is not an end in itself but rather helps ensure that incentives are aligned with the goals of model validation. While independence may be supported by separation of reporting lines, it should be judged by actions and outcomes, since there may be additional ways to ensure objectivity and prevent bias. As a practical matter, some validation work may be most effectively done by model developers and users; it is essential, however, that such validation work be subject to critical review by an independent party, who should conduct additional activities to ensure proper validation. Overall, the quality of the process is judged by the manner in which models are subject to critical review. This could be determined by evaluating the extent and clarity of documentation, the issues identified by objective parties, and the actions taken by management to address model issues.

In addition to independence, banks can support appropriate incentives in validation through compensation practices and performance evaluation standards that are tied directly to the quality of model validations and the degree of critical, unbiased review. In addition, corporate culture plays a role if it establishes support for objective thinking and encourages questioning and challenging of decisions.

Staff doing validation should have the requisite knowledge, skills, and expertise. A high level of technical expertise may be needed because of the complexity of many models, both in structure and in application. These staff also should have a significant degree of familiarity with the line of business using the model and the model's intended use. A model's developer is an important source of information but cannot be relied on as an objective or sole source on which to base an assessment of model quality.

Staff conducting validation work should have explicit authority to challenge developers and users and to elevate their findings, including issues and deficiencies. The individual or unit to whom those staff report should have sufficient influence or stature within the bank to ensure that any issues and deficiencies are appropriately addressed in a timely and substantive manner. Such influence can be reflected in reporting lines, title, rank, or designated responsibilities. Influence may be demonstrated by a pattern of actual instances in which models, or the use of models, have been appropriately changed as a result of validation.

The range and rigor of validation activities conducted prior to first use of a model should be in line with the potential risk presented by use of the model. If significant deficiencies are noted as a result of the validation process, use of the model should not be allowed or should be permitted only under very tight constraints until those issues are resolved. If the deficiencies are too severe to be addressed within the model's

framework, the model should be rejected. If it is not feasible to conduct necessary validation activities prior to model use because of data paucity or other limitations, that fact should be documented and communicated in reports to users, senior management, and other relevant parties. In such cases, the uncertainty about the results that the model produces should be mitigated by other compensating controls. This is particularly applicable to new models and to the use of existing models in new applications.

Validation activities should continue on an ongoing basis after a model goes into use, to track known model limitations and to identify any new ones. Validation is an important check on model use during periods of benign economic and financial conditions, when estimates of risk and potential loss can become overly optimistic, and when the data at hand may not fully reflect more stressed conditions. Ongoing validation activities help to ensure that changes in markets, products, exposures, activities, clients, or business practices do not create new model limitations. For example, if credit risk models do not incorporate underwriting changes in a timely manner, flawed and costly business decisions could be made before deterioration in model performance becomes apparent.

Banks should conduct a periodic review—at least annually but more frequently if warranted—of each model to determine whether it is working as intended and if the existing validation activities are sufficient. Such a determination could simply affirm previous validation work, suggest updates to previous validation activities, or call for additional validation activities. Material changes to models should also be subject to validation. It is generally good practice for banks to ensure that all models undergo the full validation process, as described in the following section, at some fixed interval, including updated documentation of all activities.

Effective model validation helps reduce model risk by identifying model errors, corrective actions, and appropriate use. It also provides an assessment of the reliability of a given model, based on its underlying assumptions, theory, and methods. In this way, it provides information about the source and extent of model risk. Validation also can reveal deterioration in model performance over time and can set thresholds for acceptable levels of error, through analysis of the distribution of outcomes around expected or predicted values. If outcomes fall consistently outside this acceptable range, then the models should be redeveloped.

2126.0.5.1 Key Elements of Comprehensive Validation

An effective validation framework should include three core elements:

- Evaluation of conceptual soundness, including developmental evidence
- Ongoing monitoring, including process verification and benchmarking
- Outcomes analysis, including back-testing

2126.0.5.1.1 Evaluation of Conceptual Soundness

This first element involves assessing the quality of the model design and construction. It entails review of documentation and empirical evidence supporting the methods used and variables selected for the model. Documentation and testing should convey an understanding of model limitations and assumptions. Validation should ensure that judgment exercised in model design and construction is well informed, carefully considered, and consistent with published research and with sound industry practice. Developmental evidence should be reviewed before a model goes into use and also as part of the ongoing validation process, in particular whenever there is a material change in the model.

A sound development process will produce documented evidence in support of all model choices, including the overall theoretical construction, key assumptions, data, and specific mathematical calculations. As part of model validation, those model aspects should be subjected to critical analysis by both evaluating the quality and extent of developmental evidence and conducting additional analysis and testing as necessary. Comparison to alternative theories and approaches should be included. Key assumptions and the choice of variables should be assessed, with analysis of their impact on model outputs and particular focus on any potential limitations. The relevance of the data used to build the model should be evaluated to ensure that it is reasonably representative of the bank's portfolio or market conditions, depending on the type of model. This is an especially important exercise when a bank uses external data or the model is used for new products or activities.

Where appropriate to the particular model, banks should employ sensitivity analysis in model development and validation to check the impact of small changes in inputs and parameter values on model outputs to make sure they fall within an expected range. Unexpectedly large changes in outputs in response to small changes in inputs can indicate an unstable model. Varying several inputs simultaneously as part of sensitivity analysis can provide evidence of unexpected interactions, particularly if the interactions are complex and not intuitively clear. Banks benefit from conducting model stress testing to check performance over a wide range of inputs and parameter values, including extreme values, to verify that the model is robust. Such testing helps establish the boundaries of model performance by identifying the acceptable range of inputs as well as conditions under which the model may become unstable or inaccurate.

Management should have a clear plan for using the results of sensitivity analysis and other quantitative testing. If testing indicates that the model may be inaccurate or unstable in some circumstances, management should consider modifying certain model properties, putting less reliance on its outputs, placing limits on model use, or developing a new approach.

Qualitative information and judgment used in model development should be evaluated, including the logic, judgment, and types of information used, to establish the conceptual soundness of the model and set appropriate conditions for its use. The validation process should ensure that qualitative, judgmental assessments are conducted in an appropriate and systematic manner, are well supported, and are documented.

2126.0.5.1.2 Ongoing Monitoring

The second core element of the validation process is ongoing monitoring. Such monitoring confirms that the model is appropriately implemented and is being used and is performing as intended.

Ongoing monitoring is essential to evaluate whether changes in products, exposures, activities, clients, or market conditions necessitate adjustment, redevelopment, or replacement of the model and to verify that any extension of the model beyond its original scope is valid. Any model limitations identified in the development stage should be regularly assessed over time, as part of ongoing monitoring. Monitoring begins when a model is first implemented in production systems for actual business use. This monitoring should continue periodically over time, with a frequency appropriate to the nature of the model, the availability of new data or modeling approaches, and the magnitude of the risk involved. Banks should design a program of ongoing testing and evaluation of model performance along with procedures for responding to any problems that appear. This program should include process verification and benchmarking.

Process verification checks that all model components are functioning as designed. It includes verifying that internal and external data inputs continue to be accurate, complete, consistent with model purpose and design, and of the highest quality available. Computer code implementing the model should be subject to rigorous quality and change control procedures to ensure that the code is correct, that it cannot be altered except by approved parties, and that all changes are logged and can be audited. System integration can be a challenge and deserves special attention because the model processing component often draws from various sources of data, processes large amounts of data, and then feeds into multiple data repositories and reporting systems. User-developed applications, such as spreadsheets or ad hoc database applications used to generate quantitative estimates, are particularly prone to model risk. As the content or composition of information changes over time, systems may need to be updated to reflect any changes in the data or its use. Reports derived from model outputs should be reviewed as part of validation to verify that they are accurate, complete, and informative, and that they contain appropriate indicators of model performance and limitations.

Many of the tests employed as part of model development should be included in ongoing monitoring and be conducted on a regular basis to incorporate additional information as it becomes available. New empirical evidence or theoretical research may suggest the need to modify or even replace original methods. Analysis of the integrity and applicability of internal and external information sources, including information provided by third-party vendors, should be performed regularly.

Sensitivity analysis and other checks for robustness and stability should likewise be repeated periodically. They can be as useful during ongoing monitoring as they are during model development. If models only work well for certain ranges of input values, market condi-

tions, or other factors, they should be monitored to identify situations where these constraints are approached or exceeded.

Ongoing monitoring should include the analysis of overrides with appropriate documentation. In the use of virtually any model, there will be cases where model output is ignored, altered, or reversed based on the expert judgment of model users. Such overrides are an indication that, in some respect, the model is not performing as intended or has limitations. Banks should evaluate the reasons for overrides and track and analyze override performance. If the rate of overrides is high, or if the override process consistently improves model performance, it is often a sign that the underlying model needs revision or redevelopment.

Benchmarking is the comparison of a given model's inputs and outputs to estimates from alternative internal or external data or models. It can be incorporated in model development as well as in ongoing monitoring. For credit-risk models, examples of benchmarks include models from vendor firms or industry consortia and data from retail credit bureaus. Pricing models for securities and derivatives often can be compared with alternative models that are more accurate or comprehensive but also too time-consuming to run on a daily basis. Whatever the source, benchmark models should be rigorous, and benchmark data should be accurate and complete to ensure a reasonable comparison.

Discrepancies between the model output and benchmarks should trigger investigation into the sources and degree of the differences, and examination of whether they are within an expected or appropriate range given the nature of the comparison. The results of that analysis may suggest revisions to the model. However, differences do not necessarily indicate that the model is in error. The benchmark itself is an alternative prediction, and the differences may be due to the different data or methods used. If the model and the benchmark match well, that is evidence in favor of the model, but it should be interpreted with caution so the bank does not get a false degree of comfort.

2126.0.5.1.3 Outcomes Analysis

The third core element of the validation process is outcomes analysis, a comparison of model outputs to corresponding actual outcomes. The precise nature of the comparison depends on the objectives of a model and might include an assessment of the accuracy of estimates or forecasts, an evaluation of rank-ordering ability, or other appropriate tests. In all cases, such comparisons help to evaluate model performance by establishing expected ranges for those actual outcomes in relation to the intended objectives and assessing the reasons for observed variation between the two. If outcomes analysis produces evidence of poor performance, the bank should take action to address those issues. Outcomes analysis typically relies on statistical tests or other quantitative measures. It can also include expert judgment to check the intuition behind the outcomes and confirm that the results make sense. When a model itself relies on expert judgment, quantitative outcomes analysis helps to evaluate the quality of that judgment. Outcomes analysis should be conducted on an ongoing basis to test whether the model continues to perform in line with design objectives and business uses.

A variety of quantitative and qualitative testing and analytical techniques can be used in outcomes analysis. The choice of technique should be based on the model's methodology, and its complexity, data availability, and the magnitude of potential model risk to the bank. Outcomes analysis should involve a range of tests because any individual test will have weaknesses. For example, some tests are better at checking a model's ability to rank-order or segment observations on a relative basis, whereas others are better at checking absolute forecast accuracy. Tests should be designed for each situation, as not all will be effective or feasible in every circumstance, and attention should be paid to choosing the appropriate type of outcomes analysis for a particular model.

Models are regularly adjusted to take into account new data or techniques, or because of deterioration in performance. Parallel outcomes analysis, under which both the original and adjusted models' forecasts are tested against realized outcomes, provides an important test of such model adjustments. If the adjusted model does not outperform the original model, developers, users, and reviewers should realize that additional changes—or even a wholesale redesign—are likely necessary before the adjusted model replaces the original one.

Back-testing is one form of outcomes analysis; specifically, it involves the comparison of actual outcomes with model forecasts during a sample time period not used in model development and at an observation frequency that matches the forecast horizon or performance window of the model. The

comparison is generally done using expected ranges or statistical confidence intervals around the model forecasts. When outcomes fall outside those intervals, the bank should analyze the discrepancies and investigate the causes that are significant in terms of magnitude or frequency. The objective of the analysis is to determine whether differences stem from the omission of material factors from the model, whether they arise from errors with regard to other aspects of model specification such as interaction terms or assumptions of linearity, or whether they are purely random and thus consistent with acceptable model performance. Analysis of in-sample fit and of model performance in holdout samples (data set aside and not used to estimate the original model) are important parts of model development but are not substitutes for back-testing.

A well-known example of back-testing is the evaluation of value-at-risk (VaR), in which actual profit and loss is compared with a model forecast loss distribution. Significant deviation in expected versus actual performance and unexplained volatility in the profits and losses of trading activities may indicate that hedging and pricing relationships are not adequately measured by a given approach. Along with measuring the frequency of losses in excess of a single VaR percentile estimator, banks should use other tests, such as assessing any clustering of exceptions and checking the distribution of losses against other estimated percentiles.

Analysis of the results of even high-quality and well-designed back-testing can pose challenges, since it is not a straightforward, mechanical process that always produces unambiguous results. The purpose is to test the model, not individual forecast values. Back-testing may entail analysis of a large number of forecasts over different conditions at a point in time or over multiple time periods. Statistical testing is essential in such cases, yet such testing can pose challenges in both the choice of appropriate tests and the interpretation of results; banks should support and document both the choice of tests and the interpretation of results.

Models with long forecast horizons should be back-tested, but given the amount of time it would take to accumulate the necessary data, that testing should be supplemented by evaluation over shorter periods. Banks should employ outcomes analysis consisting of ''early warning'' metrics designed to measure performance beginning very shortly after model introduction and trend analysis of performance over time. These outcomes analysis tools are not substitutes for back-testing, which should still be performed over the longer time period, but rather are very important complements.

Outcomes analysis and the other elements of the validation process may reveal significant errors or inaccuracies in model development or outcomes that consistently fall outside the bank's predetermined thresholds of acceptability. In such cases, model adjustment, recalibration, or redevelopment is warranted. Adjustments and recalibration should be governed by the principle of conservatism and should undergo independent review.

Material changes in model structure or technique, and all model redevelopment, should be subject to validation activities of appropriate range and rigor before implementation. At times, banks may have a limited ability to use key model validation tools like back-testing or sensitivity analysis for various reasons, such as lack of data or of price observability. In those cases, even more attention should be paid to the model's limitations when considering the appropriateness of model usage, and senior management should be fully informed of those limitations when using the models for decision making. Such scrutiny should be applied to individual models and models in the aggregate.

2126.0.5.2 Validation of Vendor and Other Third-Party Products

The widespread use of vendor and other third-party products—including data, parameter values, and complete models—poses unique challenges for validation and other model risk-management activities because the modeling expertise is external to the user and because some components are considered proprietary. Vendor products should nevertheless be incorporated into a bank's broader model risk-management framework, following the same principles as applied to in-house models, although the process may be somewhat modified.

As a first step, banks should ensure that there are appropriate processes in place for selecting vendor models. Banks should require the vendor to provide developmental evidence explaining the product components, design, and intended use, to determine whether the model is appropriate for the bank's products, exposures, and risks. Vendors should provide appropriate testing results that show their product works as expected. They should also clearly indicate the

model's limitations and assumptions and where the product's use may be problematic. Banks should expect vendors to conduct ongoing performance monitoring and outcomes analysis, with disclosure to their clients, and to make appropriate modifications and updates over time.

Banks are expected to validate their own use of vendor products. External models may not allow full access to computer coding and implementation details, so the bank may have to rely more on sensitivity analysis and benchmarking. Vendor models are often designed to provide a range of capabilities and so may need to be customized by a bank for its particular circumstances. A bank's customization choices should be documented and justified as part of validation. If vendors provide input data or assumptions, or use them to build models, their relevance for the bank's situation should be investigated. Banks should obtain information regarding the data used to develop the model and assess the extent to which that data are representative of the bank's situation. The bank also should conduct ongoing monitoring and outcomes analysis of vendor model performance using the bank's own outcomes.

Systematic procedures for validation help the bank to understand the vendor product and its capabilities, applicability, and limitations. Such detailed knowledge is necessary for basic controls of bank operations. It is also very important for the bank to have as much knowledge in-house as possible, in case the vendor or the bank terminates the contract for any reason, or if the vendor is no longer in business. Banks should have contingency plans for instances when the vendor model is no longer available or cannot be supported by the vendor.

2126.0.6 GOVERNANCE, POLICIES, AND CONTROLS—PART VI

Developing and maintaining strong governance, policies, and controls over the model risk-management framework is fundamentally important to its effectiveness. Even if model development, implementation, use, and validation are satisfactory, a weak governance function will reduce the effectiveness of overall model risk management. A strong governance framework provides explicit support and structure to risk-management functions through policies defining relevant risk-management activities, procedures that implement those policies, allocation of resources, and mechanisms for evaluating whether policies and procedures are being carried out as specified. Notably, the extent and sophistication of a bank's governance function is expected to align with the extent and sophistication of model usage.

2126.0.6.1 Board of Directors and Senior Management

Model risk governance is provided at the highest level by the board of directors and senior management when they establish a bank-wide approach to model risk management. As part of their overall responsibilities, a bank's board and senior management should establish a strong model risk-management framework that fits into the broader risk management of the organization. That framework should be grounded in an understanding of model risk—not just for individual models but also in the aggregate. The framework should include standards for model development, implementation, use, and validation.

While the board is ultimately responsible, it generally delegates to senior management the responsibility for executing and maintaining an effective model risk-management framework. Duties of senior management include establishing adequate policies and procedures and ensuring compliance, assigning competent staff, overseeing model development and implementation, evaluating model results, ensuring effective challenge, reviewing validation and internal audit findings, and taking prompt remedial action when necessary. In the same manner as for other major areas of risk, senior management, directly and through relevant committees, is responsible for regularly reporting to the board on significant model risk, from individual models and in the aggregate, and on compliance with policy. Board members should ensure that the level of model risk is within their tolerance and should direct changes where appropriate. These actions will set the tone for the whole organization about the importance of model risk and the need for active model risk management.

2126.0.6.2 Policies and Procedures

Consistent with good business practices and existing supervisory expectations, banks should formalize model risk-management activities with policies and the procedures to implement

them. Model risk-management policies should be consistent with this guidance and also be commensurate with the bank's relative complexity, business activities, corporate culture, and overall organizational structure. The board or its delegates should approve model risk-management policies and review them annually to ensure consistent and rigorous practices across the organization. Those policies should be updated as necessary to ensure that model risk-management practices remain appropriate and keep current with changes in market conditions, bank products and strategies, bank exposures and activities, and practices in the industry. All aspects of model risk management should be covered by suitable policies, including model and model risk definitions; assessment of model risk; acceptable practices for model development, implementation, and use; appropriate model validation activities; and governance and controls over the model risk-management process.

Policies should emphasize testing and analysis and promote the development of targets for model accuracy, standards for acceptable levels of discrepancies, and procedures for review of, and response to, unacceptable discrepancies. They should include a description of the processes used to select and retain vendor models, including the people who should be involved in such decisions.

The prioritization, scope, and frequency of validation activities should be addressed in these policies. They should establish standards for the extent of validation that should be performed before models are put into production and the scope of ongoing validation. The policies should also detail the requirements for validation of vendor models and third-party products. Finally, they should require maintenance of detailed documentation of all aspects of the model risk-management framework, including an inventory of models in use, results of the modeling and validation processes, and model issues and their resolution.

Policies should identify the roles and assign responsibilities within the model risk-management framework with clear detail on staff expertise, authority, reporting lines, and continuity. They should also outline controls on the use of external resources for validation and compliance and specify how that work will be integrated into the model risk-management framework.

2126.0.6.3 Roles and Responsibilities

Conceptually, the roles in model risk management can be divided among ownership, controls, and compliance. While there are several ways in which banks can assign the responsibilities associated with these roles, it is important that reporting lines and incentives be clear, with potential conflicts of interest identified and addressed.

Business units are generally responsible for the model risk associated with their business strategies. The role of model owner involves ultimate accountability for model use and performance within the framework set by bank policies and procedures. Model owners should be responsible for ensuring that models are properly developed, implemented, and used. The model owner should also ensure that models in use have undergone appropriate validation and approval processes, promptly identify new or changed models, and provide all necessary information for validation activities.

Model risk taken by business units should be controlled. The responsibilities for risk controls may be assigned to individuals, committees, or a combination of the two, and include risk measurement, limits, and monitoring. Other responsibilities include managing the independent validation and review process to ensure that effective challenge takes place. Appropriate resources should be assigned for model validation and for guiding the scope and prioritization of work. Issues and problems identified through validation and other forms of oversight should be communicated by risk-control staff to relevant individuals and business users throughout the organization, including senior management, with a plan for corrective action. Control staff should have the authority to restrict the use of models and monitor any limits on model usage. While they may grant exceptions to typical procedures of model validation on a temporary basis, that authority should be subject to other control mechanisms, such as timelines for completing validation work and limits on model use.

Compliance with policies is an obligation of model owners and risk-control staff, and there should be specific processes in place to ensure that these roles are being carried out effectively and in line with policy. Documentation and tracking of activities surrounding model development, implementation, use, and validation are needed to provide a record that makes compliance with policy transparent.

2126.0.6.4 Internal Audit

A bank's internal audit function should assess the overall effectiveness of the model risk-management framework, including the framework's ability to address both types of model risk for individual models and in the aggregate. Findings from internal audit related to models should be documented and reported to the board or its appropriately delegated agent. Banks should ensure that internal audit operates with the proper incentives, has appropriate skills, and has adequate stature in the organization to assist in model risk management. Internal audit's role is not to duplicate model risk-management activities. Instead, its role is to evaluate whether model risk management is comprehensive, rigorous, and effective. To accomplish this evaluation, internal audit staff should possess sufficient expertise in relevant modeling concepts as well as their use in particular business lines. If some internal audit staff perform certain validation activities, then they should not be involved in the assessment of the overall model risk-management framework.

Internal audit should verify that acceptable policies are in place and that model owners and control groups comply with those policies. Internal audit should also verify records of model use and validation to test whether validations are performed in a timely manner and whether models are subject to controls that appropriately account for any weaknesses in validation activities. Accuracy and completeness of the model inventory should be assessed. In addition, processes for establishing and monitoring limits on model usage should be evaluated. Internal audit should determine whether procedures for updating models are clearly documented and test whether those procedures are being carried out as specified. Internal audit should check that model owners and control groups are meeting documentation standards, including risk reporting. Additionally, internal audit should perform assessments of supporting operational systems and evaluate the reliability of data used by models.

Internal audit also has an important role in ensuring that validation work is conducted properly and that appropriate effective challenge is being carried out. It should evaluate the objectivity, competence, and organizational standing of the key validation participants, with the ultimate goal of ascertaining whether those participants have the right incentives to discover and report deficiencies. Internal audit should review validation activities conducted by internal and external parties with the same rigor to see if those activities are being conducted in accordance with this guidance.

2126.0.6.5 External Resources

Although model risk management is an internal process, a bank may decide to engage external resources to help execute certain activities related to the model risk-management framework. These activities could include model validation and review, compliance functions, or other activities in support of internal audit. These resources may provide added knowledge and another level of critical and effective challenge, which may improve the internal model development and risk-management processes. However, this potential benefit should be weighed against the added costs for such resources and the added time that external parties require to understand internal data, systems, and other relevant bank-specific circumstances.

Whenever external resources are used, the bank should specify the activities to be conducted in a clearly written and agreed-upon scope of work. A designated internal party from the bank should be able to understand and evaluate the results of validation and risk-control activities conducted by external resources. The internal party is responsible for verifying that the agreed upon scope of work has been completed; evaluating and tracking identified issues and ensuring they are addressed; and making sure that completed work is incorporated into the bank's overall model risk-management framework. If the external resources are only utilized to do a portion of validation or compliance work, the bank should coordinate internal resources to complete the full range of work needed. The bank should have a contingency plan in case an external resource is no longer available or is unsatisfactory.

2126.0.6.6 Model Inventory

Banks should maintain a comprehensive set of information for models implemented for use, under development for implementation, or recently retired. While each line of business may maintain its own inventory, a specific party should also be charged with maintaining a firm-wide inventory of all models, which should assist a bank in evaluating its model risk in the aggregate. Any variation of a model that war-

rants a separate validation should be included as a separate model and cross-referenced with other variations.

While the inventory may contain varying levels of information, given different model complexity and the bank's overall level of model usage, the following are some general guidelines. The inventory should describe the purpose and products for which the model is designed, actual or expected usage, and any restrictions on use. It is useful for the inventory to list the type and source of inputs used by a given model and underlying components (which may include other models), as well as model outputs and their intended use. It should also indicate whether models are functioning properly, provide a description of when they were last updated, and list any exceptions to policy. Other items include the names of individuals responsible for various aspects of the model development and validation; the dates of completed and planned validation activities; and the time frame during which the model is expected to remain valid.

2126.0.6.7 Documentation

Without adequate documentation, model risk assessment and management will be ineffective. Documentation of model development and validation should be sufficiently detailed so that parties unfamiliar with a model can understand how the model operates, its limitations, and its key assumptions. Documentation provides for continuity of operations, makes compliance with policy transparent, and helps track recommendations, responses, and exceptions. Developers, users, control and compliance units, and supervisors are all served by effective documentation. Banks can benefit from advances in information and knowledge management systems and electronic documentation to improve the organization, timeliness, and accessibility of the various records and reports produced in the model risk-management process.

Documentation takes time and effort, and model developers and users who know the models well may not appreciate its value. Banks should therefore provide incentives to produce effective and complete model documentation. Model developers should have responsibility during model development for thorough documentation, which should be kept up-to-date as the model and application environment changes. In addition, the bank should ensure that other participants in model risk-management activities document their work, including ongoing monitoring, process verification, benchmarking, and outcomes analysis. Also, line of business or other decision makers should document information leading to selection of a given model and its subsequent validation. For cases in which a bank uses models from a vendor or other third party, it should ensure that appropriate documentation of the third-party approach is available so that the model can be appropriately validated.

Validation reports should articulate model aspects that were reviewed, highlighting potential deficiencies over a range of financial and economic conditions, and determining whether adjustments or other compensating controls are warranted. Effective validation reports include clear executive summaries, with a statement of model purpose and an accessible synopsis of model and validation results, including major limitations and key assumptions.

2126.0.7 CONCLUSION—PART VII

This section provides comprehensive guidance on effective model risk management. Many of the activities described are common industry practice. But all banks should confirm that their practices conform to the principles in this guidance for model development, implementation, and use, as well as model validation. Banks should also ensure that they maintain strong governance and controls to help manage model risk, including internal policies and procedures that appropriately reflect the risk-management principles described in this guidance. Details of model risk-management practices may vary from bank to bank, as practical application of this guidance should be commensurate with a bank's risk exposures, its business activities, and the extent and complexity of its model use.

WHAT'S NEW IN THIS REVISED SECTION

Effective January 2013, this section was revised to acknowledge and to include minor changes relating to the issuance of SR-12-15, "Investing in Securities without Reliance on Nationally Recognized Statistical Rating Organizations," and its OCC attachment . (See section 2126.2 of this manual.) The section also updates the cited accounting standards references.

2126.1.0 SOUND RISK-MANAGEMENT PRACTICES FOR PORTFOLIO INVESTMENT

On April 23, 1998, the Federal Financial Institutions Examination Council (FFIEC) issued a Supervisory Policy Statement on Investment Securities and End-User Derivatives Activities that became effective on May 25, 1998. The statement was adopted by the Board of Governors and provides guidance on sound practices for managing the risks of investment activities. The guidance focuses on risk-management practices of state member banks and Edge corporations. The basic principles also apply to bank holding companies, which should manage and control risk exposures on a consolidated basis, recognizing the legal distinctions and potential obstacles to cash movements among subsidiaries. The statement's risk-management principles should also be incorporated into the policies of U.S. branches and agencies of foreign banks.[1]

The statement's principles set forth sound risk-management practices that are relevant to most portfolio-management endeavors. The statement places greater emphasis on a risk-focused approach to supervision. Instruments held for end-user reasons are considered, taking into consideration a variety of factors such as management's ability to manage and measure risk within the institution's holdings and the impact of those holdings on aggregate portfolio risk.

The statement focuses on managing the market, credit, liquidity, operational, and legal risks of investment and end-user activities. When managing the interest-rate-risk component of market risk, institutions are informed of the merits of developing internal policies that specify the type of pre-acquisition analysis (stress testing) that is consistent with the scope, sophistication, and complexity of their investment securities and end-user derivative holdings. Such analyses should be conducted for certain types of instruments, including those that have complex or potentially volatile risk profiles. Institutions are advised to periodically monitor the price sensitivity of their portfolios, ensuring that they meet the established limits of the board of directors. Institutions are further advised to fully assess the creditworthiness of their counterparties, including brokers and issuers. Institutions are to ensure that they take proper account of the liquidity of the instruments held. (See SR-98-12.)

2126.1.1 SUPERVISORY POLICY STATEMENT ON INVESTMENT SECURITIES AND END-USER DERIVATIVES ACTIVITIES

2126.1.1.1 Purpose

This policy statement (statement) provides guidance to financial institutions (institutions) on sound practices for managing the risks of investment securities and end-user derivatives activities.[2] The FFIEC agencies—the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the National Credit Union Administration—believe that effective management of the risks associated with securities and derivative instruments represents an essential component of safe and sound practices. This guidance describes the practices that a prudent manager normally would follow and is not intended to be a checklist. Management should establish practices and maintain documentation appropriate to the institution's individual circumstances, consistent with this statement.

1. Appropriate adaptations should be made to reflect the fact that (1) those offices are an integral part of a foreign bank that must also manage its consolidated risks and recognize possible obstacles to cash movement among branches and (2) the foreign bank is subject to overall supervision by its home-country supervisory authority.

2. The 1998 statement does not supersede any other requirements of the respective agencies' statutory rules, regulations, policies, or supervisory guidance.

2126.1.1.2 Scope

This guidance applies to all securities in *held-to-maturity* and *available-for-sale* accounts. See FASB Accounting Standards Codification section 320-10-35, ''Investment Debt and Equity Securities—Overall—Subsequent Measurement'' (formerly FAS 115, *''Accounting for Certain Debt and Equity Securities''*). It also applies to certificates of deposit held for investment purposes, and end-user derivative contracts not held in trading accounts. This guidance covers all securities used for investment purposes, including money market instruments, fixed-rate and floating-rate notes and bonds, structured notes, mortgage pass-through and other asset-backed securities, and mortgage-derivative products. Similarly, this guidance covers all end-user derivative instruments used for nontrading purposes, such as swaps, futures, and options.[3] This statement applies to all federally insured commercial banks, savings banks, savings associations, and federally chartered credit unions.

As a matter of sound practice, institutions should have programs to manage the market, credit, liquidity, legal, operational, and other risks of investment securities and end-user derivatives activities (investment activities). While risk-management programs will differ among institutions, there are certain elements that are fundamental to all sound risk-management programs. These elements include board and senior management oversight and a comprehensive risk-management process that effectively identifies, measures, monitors, and controls risk. This statement describes sound principles and practices for managing and controlling the risks associated with investment activities.

Institutions should fully understand and effectively manage the risks inherent in their investment activities. *Failure to understand and adequately manage the risks in these areas constitutes an unsafe and unsound practice.*

2126.1.1.3 Board and Senior Management Oversight

Board of director and senior management oversight is an integral part of an effective risk-management program. The board of directors is responsible for approving major policies for conducting investment activities, including the establishment of risk limits. The board should ensure that management has the requisite skills to manage the risks associated with such activities. To properly discharge its oversight responsibilities, the board should review portfolio activity and risk levels, and require management to demonstrate compliance with approved risk limits. Boards should have an adequate understanding of investment activities. Boards that do not should obtain professional advice to enhance its understanding of investment-activity oversight, so as to enable it to meet its responsibilities under this statement.

Senior management is responsible for the daily management of an institution's investments. Management should establish and enforce policies and procedures for conducting investment activities. Senior management should have an understanding of the nature and level of various risks involved in the institution's investments and how such risks fit within the institution's overall business strategies. Management should ensure that the risk-management process is commensurate with the size, scope, and complexity of the institution's holdings. Management should also ensure that the responsibilities for managing investment activities are properly segregated to maintain operational integrity. Institutions with significant investment activities should ensure that back-office, settlement, and transaction-reconciliation responsibilities are conducted and managed by personnel who are independent of those initiating risk-taking positions.

2126.1.1.4 Risk-Management Process

An effective risk-management process for investment activities includes (1) policies, procedures, and limits; (2) the identification, measurement, and reporting of risk exposures; and (3) a system of internal controls.

2126.1.1.4.1 Policies, Procedures, and Limits

Investment policies, procedures, and limits provide the structure to effectively manage investment activities. Policies should be consistent

3. Natural-person federal credit unions are not permitted to purchase nonresidential mortgage asset-backed securities and may participate in derivative programs only if authorized by the National Credit Union Administration.

with the organization's broader business strategies, capital adequacy, technical expertise, and risk tolerance. Policies should identify relevant investment objectives, constraints, and guidelines for the acquisition and ongoing management of securities and derivative instruments. Potential investment objectives include generating earnings, providing liquidity, hedging risk exposures, taking risk positions, modifying and managing risk profiles, managing tax liabilities, and meeting pledging requirements, if applicable. Policies should also identify the risk characteristics of permissible investments and should delineate clear lines of responsibility and authority for investment activities.

An institution's management should understand the risks and cash-flow characteristics of its investments. This is particularly important for products that have unusual, leveraged, or highly variable cash flows. An institution should not acquire a material position in an instrument until senior management and all relevant personnel understand and can manage the risks associated with the product.

An institution's investment activities should be fully integrated into any institution-wide risk limits. In so doing, some institutions rely only on the institution-wide limits, while others may apply limits at the investment portfolio, subportfolio, or individual instrument level.

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

2126.1.1.4.2 Risk Identification, Measurement, and Reporting

Institutions should ensure that they identify and measure the risks associated with individual transactions prior to acquisition and periodically after purchase. This can be done at the institutional, portfolio, or individual-instrument level. Prudent management of investment activities entails examination of the risk profile of a particular investment in light of its impact on the risk profile of the institution. To the extent practicable, institutions should measure exposures to each type of risk, and these measurements should be aggregated and integrated with similar exposures arising from other business activities to obtain the institution's overall risk profile.

In measuring risks, institutions should conduct their own in-house pre-acquisition analyses, or to the extent possible, make use of specific third-party analyses that are independent of the seller or counterparty. Irrespective of any responsibility, legal or otherwise, assumed by a dealer, counterparty, or financial advisor regarding a transaction, the acquiring institution is ultimately responsible for the appropriate personnel understanding and managing the risks of the transaction.

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. Reports to management should generally reflect more detail than reports to the board of the institution. 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.

2126.1.1.4.3 Internal Controls

An institution's internal control structure is critical to the safe and sound functioning of the organization generally and the management of investment activities in particular. A system of internal controls promotes efficient operations; reliable financial and regulatory reporting; and compliance with relevant laws, regulations, and institutional policies. An effective system of internal controls includes enforcing official lines of authority, maintaining appropriate separation of duties, and conducting independent reviews of investment activities.

For institutions with significant investment activities, internal and external audits are integral to the implementation of a risk-management process to control risks in investment activities. An institution should conduct periodic independent reviews of its risk-management program to ensure its integrity, accuracy, and reasonableness. Items that should be reviewed include—

1. compliance with and the appropriateness of investment policies, procedures, and limits;
2. the appropriateness of the institution's risk-measurement system given the nature, scope, and complexity of its activities; and
3. the timeliness, integrity, and usefulness of reports to the board of directors and senior management.

The review should note exceptions to policies, procedures, and limits and suggest corrective actions. The findings of such reviews should be reported to the board and corrective actions taken on a timely basis.

The accounting systems and procedures used for public and regulatory reporting purposes are critically important to the evaluation of an organization's risk profile and the assessment of its financial condition and capital adequacy. Accordingly, an institution's policies should provide clear guidelines regarding the reporting treatment for all securities and derivatives holdings. This treatment should be consistent with the organization's business objectives, generally accepted accounting principles (GAAP), and regulatory reporting standards.

2126.1.1.5 Risks of Investment Activities

The following discussion identifies particular sound practices for managing the specific risks involved in investment activities. In addition to these sound practices, institutions should follow any specific guidance or requirements from their primary supervisor related to these activities.

2126.1.1.5.1 Market Risk

Market risk is the risk to an institution's financial condition resulting from adverse changes in the value of its holdings arising from movements in interest rates, foreign-exchange rates, equity prices, or commodity prices. An institution's exposure to market risk can be measured by assessing the effect of changing rates and prices on either the earnings or economic value of an individual instrument, a portfolio, or the entire institution. For most institutions, the most significant market risk of investment activities is interest-rate risk.

Investment activities may represent a significant component of an institution's overall interest-rate-risk profile. It is a sound practice for institutions to manage interest-rate risk on an institution-wide basis. This sound practice includes monitoring the price sensitivity of the institution's investment portfolio (changes in the investment portfolio's value over different interest-rate/yield curve scenarios). Consistent with agency guidance, institutions should specify institution-wide interest-rate-risk limits that appropriately account for these activities and the strength of the institution's capital position. These limits are generally established for economic value or earnings exposures. Institutions may find it useful to establish price-sensitivity limits on their investment portfolio or on individual securities. These sub-institution limits, if established, should also be consistent with agency guidance.

It is a sound practice for an institution's management to fully understand the market risks associated with investment securities and derivative instruments prior to acquisition and on an ongoing basis. Accordingly, institutions should have appropriate policies to ensure such understanding. In particular, institutions should have policies that specify the types of market-risk analyses that should be conducted for various types or classes of instruments, including that conducted prior to their acquisition (pre-purchase analysis) and on an ongoing basis. Policies should also specify any required documentation needed to verify the analysis.

It is expected that the substance and form of such analyses will vary with the type of instrument. Not all investment instruments may need to be subjected to a pre-purchase analysis. Relatively simple or standardized instruments, the risks of which are well known to the institution, would likely require no or significantly less analysis than would more volatile, complex instruments.[4]

For relatively more complex instruments, less familiar instruments, and potentially volatile instruments, institutions should fully address pre-purchase analyses in their policies. Price-sensitivity analysis is an effective way to perform the pre-purchase analysis of individual instruments. For example, a pre-purchase analysis should show the impact of an immediate parallel shift in the yield curve of plus and minus 100, 200, and 300 basis points. Where appropriate, such analysis should encompass a wider range of scenarios, including nonparallel changes in the yield curve. A comprehensive analysis may also take into account other relevant factors, such as changes in interest-rate volatility and changes in credit spreads.

When the incremental effect of an investment position is likely to have a significant effect on the risk profile of the institution, it is a sound practice to analyze the effect of such a position on the overall financial condition of the institution.

Accurately measuring an institution's market risk requires timely information about the cur-

4. Federal credit unions must comply with the investment-monitoring requirements of 12 C.F.R. 703.90. See 62 *Fed. Reg.* 32,989 (June 18, 1997).

rent carrying and market values of its investments. Accordingly, institutions should have market-risk-measurement systems commensurate with the size and nature of these investments. Institutions with significant holdings of highly complex instruments should ensure that they have the means to value their positions. Institutions employing internal models should have adequate procedures to validate the models and to periodically review all elements of the modeling process, including its assumptions and risk-measurement techniques. Managements relying on third parties for market-risk-measurement systems and analyses should ensure that they fully understand the assumptions and techniques used.

Institutions should provide reports to their boards on the market-risk exposures of their investments on a regular basis. To do so, the institution may report the market-risk exposure of the whole institution. Alternatively, reports should contain evaluations that assess trends in aggregate market-risk exposure and the performance of portfolios in terms of established objectives and risk constraints. They also should identify compliance with board-approved limits and identify any exceptions to established standards. Institutions should have mechanisms to detect and adequately address exceptions to limits and guidelines. Management reports on market risk should appropriately address potential exposures to yield curve changes and other factors pertinent to the institution's holdings.

2126.1.1.5.2 Credit Risk

Broadly defined, credit risk is the risk that an issuer or counterparty will fail to perform on an obligation to the institution. For many financial institutions, credit risk in the investment portfolio may be low relative to other areas, such as lending. However, this risk, as with any other risk, should be effectively identified, measured, monitored, and controlled.

An institution should not acquire investments or enter into derivative contracts without assessing the creditworthiness of the issuer or counterparty. The credit risk arising from these positions should be incorporated into the overall credit-risk profile of the institution as comprehensively as practicable. Institutions are to meet certain creditworthiness standards for security purchases. Many institutions may maintain and update internal credit-rating reports and assessments that can be supplemented by reports from major external credit-rating services. For nonrated securities, institutions should establish guidelines to ensure that the securities meet legal requirements and that the institution fully understands the risk involved. Institutions should establish limits on individual counterparty exposures. Policies should also provide credit-risk and concentration limits. Such limits may define concentrations relating to a single or related issuer or counterparty, a geographical area, or obligations with similar characteristics.

In managing credit risk, institutions should consider settlement and presettlement credit risk. These risks are the possibility that a counterparty will fail to honor its obligation at or before the time of settlement. The selection of dealers, investment bankers, and brokers is particularly important in effectively managing these risks. The approval process should include a review of each firm's financial statements and an evaluation of its ability to honor its commitments. An inquiry into the general reputation of the dealer is also appropriate. This includes review of information from state or federal securities regulators and industry self-regulatory organizations such as the National Association of Securities Dealers concerning any formal enforcement actions against the dealer, its affiliates, or associated personnel.

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.

Sound credit-risk management requires that credit limits be developed by personnel who are as independent as practicable of the acquisition function. In authorizing issuer and counterparty credit lines, these personnel should use standards that are consistent with those used for other activities conducted within the institution and with the organization's overall policies and consolidated exposures.

2126.1.1.5.3 Liquidity Risk

Liquidity risk is the risk that an institution cannot easily sell, unwind, or offset a particular position at a fair price because of inadequate market depth. In specifying permissible instruments for accomplishing established objectives, institutions should ensure that they take into account the liquidity of the market for those instruments and the effect that such characteristics have on achieving their objectives. The liquidity of certain types of instruments may

make them inappropriate for certain objectives. Institutions should ensure that they consider the effects that market risk can have on the liquidity of different types of instruments under various scenarios. Accordingly, institutions should articulate clearly the liquidity characteristics of instruments to be used in accomplishing institutional objectives.

Complex and illiquid instruments can often involve greater risk than actively traded, more liquid securities. Oftentimes, this higher potential risk arising from illiquidity is not captured by standardized financial modeling techniques. Such risk is particularly acute for instruments that are highly leveraged or that are designed to benefit from specific, narrowly defined market shifts. If market prices or rates do not move as expected, the demand for such instruments can evaporate, decreasing the market value of the instrument below the modeled value.

2126.1.1.5.4 Operational (Transaction) Risk

Operational (transaction) risk is the risk that deficiencies in information systems or internal controls will result in unexpected loss. Sources of operating risk include inadequate procedures, human error, system failure, or fraud. Inaccurately assessing or controlling operating risks is one of the more likely sources of problems facing institutions involved in investment activities.

Effective internal controls are the first line of defense in controlling the operating risks involved in an institution's investment activities. Of particular importance are internal controls that ensure the separation of duties and supervision of persons executing transactions from those responsible for processing contracts, confirming transactions, controlling various clearing accounts, preparing or posting the accounting entries, approving the accounting methodology or entries, and performing revaluations.

Consistent with the operational support of other activities within the financial institution, securities operations should be as independent as practicable from business units. Adequate resources should be devoted, such that systems and capacity are commensurate with the size and complexity of the institution's investment activities. Effective risk management should also include, at least, the following:

1. *Valuation.* Procedures should ensure independent portfolio pricing. For thinly traded or illiquid securities, completely independent pricing may be difficult to obtain. In such cases, operational units may need to use prices provided by the portfolio manager. For unique instruments where the pricing isbeing provided by a single source (e.g., the dealer providing the instrument), the institution should review and understand the assumptions used to price the instrument.
2. *Personnel.* The increasingly complex nature of securities available in the marketplace makes it important that operational personnel have strong technical skills. This will enable them to better understand the complex financial structures of some investment instruments.
3. *Documentation.* Institutions should clearly define documentation requirements for securities transactions, saving and safeguarding important documents, as well as maintaining possession and control of instruments purchased.

An institution's policies should also provide guidelines for conflicts of interest for employees who are directly involved in purchasing and selling securities for the institution from securities dealers. These guidelines should ensure that all directors, officers, and employees act in the best interest of the institution. The board may wish to adopt policies prohibiting these employees from engaging in personal securities transactions with these same securities firms without specific prior board approval. The board may also wish to adopt a policy applicable to directors, officers, and employees restricting or prohibiting the receipt of gifts, gratuities, or travel expenses from approved securities dealer firms and their representatives.

2126.1.1.5.5 Legal Risk

Legal risk is the risk that contracts are not legally enforceable or documented correctly. Institutions should adequately evaluate the enforceability of its agreements before individual transactions are consummated. Institutions should also ensure that the counterparty has authority to enter into the transaction and that the terms of the agreement are legally enforceable. Institutions should further ascertain that netting agreements are adequately documented, executed properly, and are enforceable in all relevant jurisdictions. Institutions should have knowledge of relevant tax laws and

interpretations governing the use of these instruments.

On November 15, 2012, state member banks were advised, effective January 1, 2013, that they may no longer rely solely on credit ratings issued by nationally recognized statistical rating organizations (NRSROs) or external credit ratings to determine whether a particular security is an ''investment security'' that is permissible for investment by a state member bank. Under the regulations of the Office of the Comptroller of the Currency (OCC), securities qualify for investment by national banks only if they are determined by the bank to be ''investment grade'' and not predominantly speculative in nature. (See SR-12-15 and its attachment.) The basic sound risk-management principles of this policy and other referenced guidance that follows also applies to bank holding companies (BHCs) and savings and loan holding companies (SLHCs). They should manage and control their risk exposures on a consolidated basis and give recognition to the legal distinctions and potential obstacles to the cash movements among their financial institution subsidiaries. Since a BHC's structure can include national banks, state member banks, and other financial institution subsidiaries, the referenced statutory, regulatory, and supervisory guidance is provided.

Under the Federal Reserve Act (12 USC 335) and the Federal Reserve (FR)'s Regulation H (12 CFR 208.21), state member banks are subject to the same limitations and conditions with respect to the purchasing, selling, underwriting, and holding of investment securities and stock as national banks under the National Banking Act (12 USC 24 (Seventh)). Therefore, when investing in securities, state member banks must comply with the provisions of the National Banking Act and the OCC regulations in 12 CFR part 1. In addition to this federal requirement, a state member bank may purchase, sell, underwrite, or hold securities and stock only to the extent permitted under applicable state law.

National banks are to assess a security's creditworthiness to determine if it is ''investment grade.'' A security meets the ''investment grade'' test only if the issuer has an adequate capacity to meet its financial commitments under the security for the projected life of the asset or exposure. Under this definition, the issuer has an adequate capacity to meet financial commitments if (1) the risk of default by the obligor is low and (2) the full and timely repayment of principal and interest is expected.[1] National banks are expected to consider a number of factors, to the extent appropriate in making this determination. While a national bank may continue to take into account external credit ratings and assessments as a valuable source of information, the bank is expected to supplement these ratings with a degree of due diligence processes and additional analyses appropriate for the bank's risk profile and for the size and complexity of the instrument.[2]

The OCC issued guidance, effective January 1, 2013 (OCC investment guidance), to clarify regulatory expectations with respect to investment purchase decisions and ongoing portfolio due diligence processes. See appendix 1 below (section 2126.2.1). The guidance clarifies that generally, investment securities are expected to have good to very strong credit quality. In the case of structured securities, this determination may be influenced more by the quality of the underlying collateral, the cash flow rules, and the structure of the security itself than by the condition of the issuer.

The OCC also expects national banks to conduct an appropriate level of due diligence to understand the inherent risks of a security and determine that it is a permissible investment. The extent of the due diligence should be sufficient to support the institution's conclusion that a security meets the ''investment-grade'' standards. The depth of the due diligence should be a function of the security's credit quality, the complexity of the structure, and the size of the investment. Third-party analytics may be part of this analysis, although the national bank's management remains responsible for the investment decision and should ensure that prospective third parties are independent, reliable, and qualified. The guidance also sets forth an expectation that the board of directors should oversee management to make sure appropriate decisionmaking processes are in place.[3]

Investment in securities and stock by state member banks are required under the Federal Reserve Act and Regulation H to comply with the revised 12 CFR part 1 and should also meet the supervisory expectations set forth in the OCC investment guidance and this FR guidance. In addition, state member banks are expected to continue to meet long-established

1. See 77 *Fed. Reg.* 35257 (June 13, 2012).

2. See 77 *Fed. Reg.* 35254 (June 13, 2012).

3. See 77 *Fed. Reg.* 35259 (June 13, 2012).

supervisory expectations for risk-management processes to ensure that the credit risk of the bank, including the credit risk of the investment portfolio, is effectively identified, measured, monitored, and controlled.

2126.2.1 APPENDIX 1—OCC GUIDANCE ON DUE DILIGENCE REQUIREMENTS IN DETERMINING WHETHER SECURITIES ARE ELIGIBLE FOR INVESTMENT

The guidance below was issued by the Office of the Comptroller of the Currency (OCC) on June 13, 2012, and is being included for ease of reference. The official guidance was published in the Federal Register (77 Fed. Reg. 35259), and is available as an attachment to OCC Bulletin 2012-18. As discussed in SR-12-15, the Federal Reserve also expects that state member banks (SMBs) will meet the supervisory expectations set forth in the OCC guidance as this guidance provides further clarification to the OCC rule with which SMBs must comply. (See 12 CFR part 1, and 77 Fed. Reg. 35253, June 13, 2012.)

Purpose

The OCC has issued final rules to revise the definition of ''investment grade,'' as that term is used in 12 CFR parts 1 and 160 in order to comply with section 939A of the Dodd-Frank Act. Institutions, effective January 1, 2013, are to ensure that existing investments comply with the revised ''investment grade'' standard, as applicable based on investment type, and safety and soundness practices described in 12 CFR 1.5 and this guidance. This implementation period also will provide management with time to evaluate and amend existing policies and practices to ensure new purchases comply with the final rules and guidance. National banks that have established due diligence review processes, and that have not relied exclusively on external credit ratings, should not have difficulty establishing compliance with the new standard.

The OCC is issuing this guidance (Guidance) to clarify steps national banks ordinarily are expected to take to demonstrate they have properly verified their investments meet the newly established credit-quality standards under 12 CFR part 1 and steps national banks are expected to take to demonstrate they are in compliance with due diligence requirements when purchasing investment securities and conducting ongoing reviews of their investment portfolios. The standards below describe how national banks may purchase, sell, deal in, underwrite, and hold securities consistent with the authority contained in 12 U.S.C. 24 (Seventh). The activities of national banks must be consistent with safe and sound banking practices, and this Guidance reminds national banks of the supervisory risk-management expectations associated with permissible investment portfolio holdings under parts 1 and 160.

Background

Parts 1 and 160 provide standards for determining whether securities have appropriate credit quality and marketability characteristics to be purchased and held by national banks. These requirements also establish limits on the amount of investment securities an institution may hold for its own account. As defined in 12 CFR part 1, an ''investment security'' must be ''investment grade.'' For the purpose of part 1, ''investment grade'' securities are those where the issuer has an adequate capacity to meet the financial commitments under the security for the projected life of the investment. An issuer has an adequate capacity to meet financial commitments if the risk of default by the obligor is low and the full and timely repayment of principal and interest is expected. Generally, securities with good to very strong credit quality will meet this standard. In the case of a structured security (that is, a security that relies primarily on the cash flows and performance of underlying collateral for repayment, rather than the credit of the entity that is the issuer), the determination that full and timely repayment of principal and interest is expected may be influenced more by the quality of the underlying collateral, the cash flow rules, and the structure of the security itself than by the condition of the issuer.

National banks must be able to demonstrate that their investment securities meet applicable credit-quality standards. This Guidance provides criteria that national banks can use in meeting part 1 credit-quality standards and that national banks can use in meeting due diligence requirements.

Determining Whether Securities Are Permissible Prior to Purchase

The OCC's elimination of references to credit ratings in its regulations, in accordance with the Dodd-Frank Act, does not substantively change the standards institutions should use when deciding whether securities are eligible for purchase under part 1. The OCC's investment securities regulations generally require a national bank to determine whether or not a security is ''investment grade'' in order to determine whether purchasing the security is permissible. Investments are considered ''investment grade'' if they meet the regulatory standard for credit quality. To meet this standard, a national bank must be able to determine that the security has (1) low risk of default by the obligor and (2) the expectation of full and timely repayment of principal and interest over the expected life of the investment.

For national banks, Type I securities, as defined in part 1, generally are government obligations and are not subject to investment grade criteria for determining eligibility to purchase. Typical Type I obligations include U.S. Treasuries, agencies, municipal government general obligations, and for well-capitalized institutions, municipal revenue bonds. While Type I obligations do not have to meet the investment grade criteria to be eligible for purchase, all investment activities should comply with safe and sound banking practices as stated in 12 CFR 1.5 and in previous regulatory guidance. Under OCC rules, Treasury and agency obligations do not require individual credit analysis, but bank management should consider how those securities fit into the overall purpose, plans, and risk and concentration limitations of the investment policies established by the board of directors. Municipal bonds should be subject to an initial credit assessment and then ongoing review consistent with the risk characteristics of the bonds and the overall risk of the portfolio.

Financial institutions should be well acquainted with fundamental credit analysis as this is central to a well-managed loan portfolio. The foundation of a fundamental credit analysis-character, capacity, collateral, and covenants-applies to investment securities just as it does to the loan portfolio. Accordingly, the OCC expects national banks to conduct an appropriate level of due diligence to understand the inherent risks and determine that a security is a permissible investment. The extent of the due diligence should be sufficient to support the institution's conclusion that a security meets the investment grade standards. This may include consideration of internal analyses, third party research and analytics including external credit ratings, internal risk ratings, default statistics, and other sources of information as appropriate for the particular security. Some institutions may have the resources to do most or all of the analytical work internally. Some, however, may choose to rely on third parties for much of the analytical work. While analytical support may be delegated to third parties, management may not delegate its responsibility for decisionmaking and should ensure that prospective third parties are independent, reliable, and qualified. The board of directors should oversee management to assure that an appropriate decisionmaking process is in place.

The depth of the due diligence should be a function of the security's credit quality, the complexity of the structure, and the size of the investment. The more complex a security's structure, the more credit-related due diligence an institution should perform, even when the credit quality is perceived to be very high. Management should ensure it understands the security's structure and how the security may perform in different default environments, and should be particularly diligent when purchasing structured securities.[4] The OCC expects national banks to consider a variety of factors relevant to the particular security when determining whether a security is a permissible and sound investment. The range and type of specific factors an institution should consider will vary depending on the particular type and nature of the securities. As a general matter, a national bank will have a greater burden to support its determination if one factor is contradicted by a finding under another factor.

The following matrix provides examples of factors for national banks to consider as part of a robust credit-risk assessment framework for designated types of instruments. The types of securities included in the matrix require a credit-focused pre-purchase analysis to meet the investment grade standard or safety and soundness standards. Again, the matrix is provided as a guide to better inform the credit-risk assessment process. Individual purchases may require more or less analysis dependent on the security's risk characteristics, as previously described.

4. For example, a national bank should be able to demonstrate an understanding of the effects on cash flows of a structured security assuming varying default levels in the underlying assets.

Key factors	Corporate bonds	Municipal government general obligations	Revenue bonds	Structured securities
Confirm spread to U.S. Treasuries is consistent with bonds of similar credit quality	X	X	X	X
Confirm risk of default is low and consistent with bonds of similar credit quality	X	X	X	X
Confirm capacity to pay and assess operating and financial performance levels and trends through internal credit analysis and/or other third party analytics, as appropriate for the particular security	X	X	X	X
Evaluate the soundness of a municipal's budgetary position and stability of its tax revenues. Consider debt profile and level of unfunded liabilities, diversity of revenue sources, taxing authority, and management experience		X		
Understand local demographics/economics. Consider unemployment data, local employers, income indices, and home values		X	X	
Assess the source and strength of revenue structure for municipal authorities. Consider obligor's financial condition and reserve levels, annual debt service and debt coverage ratio, credit enhancement, legal covenants, and nature of project			X	
Understand the class or tranche and its relative position in the securitization structure				X
Assess the position in the cash flow waterfall				X
Understand loss allocation rules, specific definition of default, the potential impact of performance and market value triggers, and support provided by credit and/or liquidity enhancements				X
Evaluate and understand the quality of the underwriting of the underlying collateral as well as any risk concentrations				X
Determine whether current underwriting is consistent with the original underwriting underlying the historical performance of the collateral and consider the effect of any changes				X
Assess the structural subordination and determine if adequate given current underwriting standards				X
Analyze and understand the impact of collateral deterioration on tranche performance and potential credit losses under adverse economic conditions				X

Additional Guidance on Structured Securities Analysis

The creditworthiness assessment for an investment security that relies on the cash flows and collateral of the underlying assets for repayment (i.e., a structured security) is inherently different from a security that relies on the financial capacity of the issuer for repayment. Therefore, a financial institution should demonstrate an understanding of the features of a structured security that would materially affect its performance and that its risk of loss is low even under adverse economic conditions. Management's assessment of key factors, such as those provided in this guidance, will be considered a critical component of any structured security evaluation. Existing OCC guidance, including OCC Bulletin 2002-19, "Supplemental Guidance, Unsafe and Unsound Investment Portfolio Practices," states that it is unsafe and unsound to purchase a complex high-yield security without an understanding of the security's structure and performing a scenario analysis that evaluates how the security will perform in different default environments. Policies that specifically permit this type of investment should establish appropriate limits, and prepurchase due diligence processes should consider the impact of such purchases on capital and earnings under a variety of possible scenarios. The OCC expects institutions to understand the effect economic stresses may have on an investment's cash flows. Various factors can be used to define the stress scenarios. For example, an institution could evaluate the potential impact of changes in economic growth, stock market movements, unemployment, and home values on default and recovery rates. Some institutions have the resources to perform this type of analytical work internally. Generally, analyses of the application of various stress scenarios to a structured security's cash flow are widely available from third parties. Many of these analyses evaluate the performance of the security in a base case and a moderate and severe stress case environment. Even under severe stress conditions, the stress scenario analysis should determine that the risk of loss is low and full and timely repayment of principal and interest is expected.

Maintaining an Appropriate and Effective Portfolio Risk-Management Framework

The OCC has had a long-standing expectation that national banks implement a risk-management process to ensure credit risk, including credit risk in the investment portfolio, is effectively identified, measured, monitored, and controlled. The *1998 Interagency Supervisory Policy Statement on Investment Securities and End-User Derivatives Activities* (Policy Statement) contains risk-management standards for the investment activities of banks and savings associations.[5] The Policy Statement emphasizes the importance of establishing and maintaining risk processes to manage the market, credit, liquidity, legal, operational, and other risks of investment securities. Other previously issued guidance that supplements OCC investment standards are OCC 2009-15, "Risk Management and Lessons Learned" (which highlights lessons learned during the market disruption and re-emphasizes the key principles discussed in previously issued OCC guidance on portfolio risk management); OCC 2004-25, "Uniform Agreement on the Classification of Securities" (which describes the importance of management's credit-risk analysis and its use in examiner decisions concerning investment security risk ratings and classifications); and OCC 2002-19, "Supplemental Guidance, Unsafe and Unsound Investment Portfolio Practices" (which alerts banks to the potential risk to future earnings and capital from poor investment decisions made during periods of low levels of interest rates and emphasizes the importance of maintaining prudent credit, interest rate, and liquidity risk-management practices to control risk in the investment portfolio).

National banks must have in place an appropriate risk-management framework for the level of risk in their investment portfolios. Failure to maintain an adequate investment portfolio risk-management process, which includes understanding key portfolio risks, is considered an unsafe and unsound practice.

Having a strong and robust risk-management framework appropriate for the level of risk in an institution's investment portfolio is particularly critical for managing portfolio credit risk. A key role for management in the oversight process is to translate the board of directors' tolerance for risk into a set of internal operating policies and procedures that govern the institution's investment activities. Policies should be consistent with the organization's broader business strategies, capital adequacy, technical expertise, and

5. On April 23, 1998, the FRB, FDIC, NCUA, and OCC issued the "Supervisory Policy Statement on Investment Securities and End-User Derivatives Activities."

risk tolerance. Institutions should ensure that they identify and measure the risks associated with individual transactions prior to acquisition and periodically after purchase. This can be done at the institutional, portfolio, or individual instrument level. Investment policies also should provide credit-risk concentration limits. Such limits may apply to concentrations relating to a single or related issuer, a geographical area, and obligations with similar characteristics. Safety-and-soundness principles warrant effective concentration risk-management programs to ensure that credit exposures do not reach an excessive level.

The aforementioned risk-management policies, principles, and due diligence processes should be commensurate with the complexity of the investment portfolio and the materiality of the portfolio to the financial performance and capital position of the institution. Investment review processes, following the pre-purchase analysis, may vary from institution to institution based on the individual characteristics of the portfolio, the nature and level of risk involved, and how that risk fits into the overall risk profile and operation of the institution. Investment portfolio reviews may be risk-based and focus on material positions or specific groups of investments or stratifications to enable analysis and review of similar risk positions.

As with pre-purchase analytics, some institutions may have the resources necessary to do most or all of their portfolio reviews internally. However, some may choose to rely on third parties for much of the analytical work. Third-party vendors offer risk analysis and data benchmarks that could be periodically reviewed against existing portfolio holdings to assess credit-quality changes over time. Holdings where current financial information or other key analytical data is unavailable should warrant more frequent analysis. High-quality investments generally will not require the same level of review as investments further down the credit-quality spectrum. However, any material positions or concentrations should be identified and assessed in more depth and more frequently, and any system should ensure an accurate and timely risk assessment and reporting process that informs the board of material changes to the risk profile and prompts action when needed. National banks should have investment portfolio review processes that effectively assess and manage the risks in the portfolio and ensure compliance with policies and risk limits. Institutions should reference existing regulatory guidance for additional supervisory expectations for investment portfolio risk-management practices.

2126.2.2 LAWS, REGULATIONS, INTERPRETATIONS, AND ORDERS

Subject	*Laws*[1]	*Regulations*[2]	*Interpretations*[3]	*Orders*
State member banks are subject to same limitations and conditions for investments activities as national banks	24 (Seventh), 335	1, 208.21		
Federal financial institution regulatory agencies to remove references to, and requirements of reliance on, external credit ratings in any regulation that requires the assessment of the creditworthiness of a security or money market instrument.	15 U.S.C. 780			
Supervisory and risk expectations		1, 160		
Safety and soundness practices		1.5		

1. 12 U.S.C., unless specifically stated otherwise.
2. 12 C.F.R., unless specifically stated otherwise.

3. *Federal Reserve Regulatory Service* reference.

Bank holding companies should directly manage and control their aggregate risk exposures on a consolidated basis and, if appropriate, for individual subsidiaries, in view of the distinct legal existence of various subsidiaries and possible obstacles to moving cash, other assets, and contractual agreements among subsidiaries.[1] See SR-99-3.

2126.3.1 FUNDAMENTAL ELEMENTS OF COUNTERPARTY CREDIT RISK MANAGEMENT

When conducting bank holding company inspections and supervisory contacts, and when monitoring trading and derivatives activities, supervisors and examiners should fully evaluate the integrity of certain key elements of a banking organization's (BO) counterparty credit risk management process, such as the following:

1. The BO's assessment of counterparty creditworthiness, both initially and on an ongoing basis. A counterparty's creditworthiness can be evidenced by its capital strength, leverage, any on- and off-balance-sheet risk factors, and contingencies. Creditworthiness can also be evidenced by the counterparty's liquidity, operating results, reputation, and ability to understand and manage the risks inherent in its line of business, as well as the risks involved in the particular products and transactions that define a particular customer relationship.
2. The standards, methodologies, and techniques used in measuring counterparty-credit-risk exposures on an individual instrument, counterparty, and portfolio basis.
3. The use and management of credit enhancements to mitigate counterparty credit risks, including collateral arrangements and collateral-management systems, contractual downgrades or material-change triggers, and contractual "option-to-terminate" or close-out provisions.
4. The risk-limit and -monitoring systems that involve (1) setting meaningful limits on counterparty credit risk, (2) monitoring exposures against those limits, and (3) initiating meaningful risk assessments and risk-controlling actions in the event that exposures exceed limits.

The confluence of competitive pressures, pursuit of earnings, and overreliance on customer reputation can lead to substantive lapses in fundamental risk-management principles regarding counterparty risk assessment, exposure monitoring, and the management of credit-risk limits. Policies governing these activities may be unduly general so as to compromise their usefulness in managing the risks involved with particular types of counterparties. Practices may not conform to the stated policies or their intent. Situations may also exist where internal controls, including documentation and independent review, may be inadequate or lack rigor. For some larger BOs, regimes for measuring and monitoring counterparty-credit-risk exposure may be effective in more traditional areas of credit extension, but may need enhancements when used in trading and derivatives activities.

2126.3.2 TARGETING SUPERVISORY RESOURCES

When risk focusing their supervisory initiatives, examiners should continue to target those activities and areas with significant growth and above-normal profitability profiles—especially in trading and derivatives activities where the press of business and competitive pressures may invite a BO to offer new product lines before the approval of counterparties and the necessary risk-management infrastructure or procedures are fully in place. Supervisors and examiners should encourage a BO to adopt growth, profitability, and size criteria for their audit and independent risk-management functions to use in targeting their reviews.

1. These basic principles are also to be employed in the supervision of U.S. branches and agencies of foreign banks, with appropriate adaptations to reflect that (1) those offices are an integral part of a foreign bank that should be managing its risks on a consolidated basis and recognizing possible obstacles to cash movements among branches, and (2) the foreign bank is subject to overall supervision by its home-country authorities.

2126.3.3 ASSESSMENT OF COUNTERPARTY CREDITWORTHINESS

Supervisors and examiners should increase their focus on the appropriateness, specificity, and rigor of the policies, procedures, and internal controls that a BO currently uses to assess the counterparty credit risks arising from its trading and derivatives activities. BOs should have extensive written policies covering their assessment of counterparty creditworthiness for both the initial due-diligence process (that is, before conducting business with a customer) and for ongoing monitoring. Examiners should focus particular attention on how such policies are structured and implemented. Broadly structured, general policies that apply to all types of counterparties may prove inadequate for directing staff in the proper review of the risks posed by particular types of counterparties. For example, although most policies call for the assessment and monitoring of the capital strength and leverage of customers, the assessment of hedge-fund counterparties should not rely exclusively on simple balance-sheet measures and traditional assessments of financial condition. This information may be insufficient for those counterparties whose off-balance-sheet positions are a source of significant leverage and whose risk profiles are narrowly based on concentrated business lines (such as with hedge funds and similar institutional investors). General policies calling for periodic counterparty credit reviews over significant intervals (such as annually) are another example of broad policies that may compromise the integrity of the assessment of individual counterparties or types of counterparties—a counterparty's risk profile can change significantly over much shorter time horizons.

Credit-risk-assessment policies should also properly define the types of analyses to be conducted for particular types of counterparties based on the nature of their risk profiles. Stress testing and scenario analysis may be needed, in addition to customizing fundamental analyses based on industry and business-line characteristics. Customized analyses are particularly important when a counterparty's creditworthiness may be adversely affected by short-term fluctuations in financial markets, especially when potential credit exposure to a counterparty increases at the same time the counterparty's credit quality deteriorates.

Examiners should continue to pay special attention to areas where banking organization practices may not conform to stated policies. Such supervisory efforts may be especially difficult when the BO's policies are not specific enough for it to properly focus its counterparty risk assessments. Therefore, examiners must ensure that the banking organization's policies sufficiently address the risk profiles of particular types of counterparties and instruments. The policies should specify (1) the types of counterparties that may require special consideration; (2) the types and frequency of information to be obtained from such counterparties; (3) the types and frequency of analyses to be conducted, including the need for and type of any stress-testing analysis; and (4) how such information and analyses appropriately address the risk profile of the particular type of counterparty. This specificity in credit-assessment policies is particularly important when limited transparency may hinder market discipline on the risk-taking activities of counterparties—as may be the case with hedge funds.

Examiners should also place increasing emphasis on ensuring that a BO's existing practice conforms both with its stated objectives and the intent of its established policies. For example, some BOs may not obtain and evaluate all the information on the financial strength, condition, and liquidity of some types of counterparties that may be required by their own policies. In highly competitive and fast-moving transaction areas, organizations should be sufficiently rigorous in conducting the analyses specified in their policies, such as the review of a counterparty's ability to manage the risks of its business.

Necessary internal controls for ensuring that practices conform with stated policies include actively enforced documentation standards and periodic independent reviews by internal auditors or other risk-control units, particularly for business lines, products, and exposures to particular groups of counterparties and individual customers that exhibit significant growth or above-normal profitability. Using targeted inspections and reviews, examiners should evaluate the integrity of a BO's internal controls. Examiners should thus conduct their own transaction testing of such situations. This testing should include robust sampling of transactions with major counterparties in the targeted area, as well as sufficient stratification to ensure that practices involving smaller relationships also adhere to stated policies.

2126.3.4 CREDIT-RISK-EXPOSURE MEASUREMENT

Financial market turbulence emphasizes the important interrelationships between market movements and the credit-risk exposures involved in derivatives activities. Accordingly, supervisors and examiners should be alert to situations where a BO may need to be more diligent in conducting current computations of the loan equivalents and potential future exposures (PFE) that are used to measure, monitor, and control its derivatives counterparty credit exposure.

Most BOs fully recognize that the credit risk of derivatives positions includes both the current replacement cost of a contract as well as the contract's PFE. PFEs are generally calculated using statistical techniques to estimate the worst potential loss over a specified time horizon at some specified confidence interval (for example, 95 percent, 97.5 percent, and 99 percent), which is generally derived in some manner from historically observed market fluctuations. Together with the current replacement cost, such PFEs are used to convert derivatives contracts to "loan equivalents" for aggregating credit exposures across products and instruments.

The time horizon used to calculate PFEs can vary depending on the banking organization's risk tolerance, collateral protection, and ability to terminate its credit exposure. Some BOs may use a time horizon equal to the life of the respective instrument. While such a time horizon may be appropriate for unsecured positions, for collateralized exposures, the use of lifetime, worst-case-estimate PFEs may be ineffective to measure the true nature of counterparty risk exposure. While life-of-contract PFE measures provide an objective and conservative long-term exposure estimate, they bear little relationship to the actual credit exposures typically incurred in the case of collateralized relationships. In such cases, a banking organization's actual credit exposure is the PFE from the time a counterparty fails to meet a collateral call until the time the bank liquidates its collateral and closes out the derivative contract—a period which is typically much shorter than the contract's life. The lack of realism in conservative measurement can cause managers and traders to discount them and may result in inappropriate limits being set, thereby compromising the entire risk-management process.

More realistic measures of collateralized credit-risk exposures should also take into account the shorter time horizons over which action can be taken to mitigate losses in times of market stress. These measures should incorporate estimates of collateral-recovery rates given the potential market liquidity impacts of stress events on collateral values. Some BOs already do stress tests, calculating measures that assess the worst-case value of positions over a time horizon of one or two weeks—their estimate of a reasonable liquidation period in times of stress. They also perform scenario analyses of counterparty credit exposures. Stress testing and scenario analyses should evaluate the impact of large market moves on the credit exposure to individual counterparties, and they should assess the implications inherent in liquidating positions under such conditions. Analyses should consider the effects of market liquidity on the value of positions and any related collateral. The use of meaningful scenario analyses is particularly important since stress tests derived from simple applications of higher confidence intervals or longer time horizons to PFE, value-at-risk, and other measures may not adequately capture the market and exposure dynamics under turbulent market conditions, particularly as they relate to the interaction between market, credit, and liquidity risk.

The results of stress testing and scenario analyses should be incorporated into senior management reports. Such reports should provide sufficient information to ensure an adequate understanding of the nature of the exposure and the analyses conducted. Information should also be sufficient to trigger risk-controlling actions where necessary.

Other BOs are moving to build the capability of estimating portfolio-based PFEs by any one of several different time horizons or buckets, depending on the liquidity and breadth of the underlying instrument or risk factor. Based on management's opinion of the appropriate workout timeframe, different time horizons can be used for different counterparties, transactions, or collateral types to more precisely define exposures. Supervisors and examiners should be alert to situations where collateralized exposures may be inaccurately estimated, and should encourage management at these BOs to enhance their exposure-measurement systems accordingly.

Supervisors should also be cognizant of the manner in which the credit exposures are aggregated for individual counterparties. Some BOs may take a purely transactional approach to aggregation and *not incorporate the netting of long and short derivatives contracts*, even when legally enforceable bilateral netting agreements

are available. In such cases, *simple sum estimates of positive exposures may seriously overestimate true credit exposure*, and examiners should monitor and encourage a BO's movement toward more realistic measures of counterparty exposure. Other BOs may take a portfolio approach, in which information systems allow and incorporate netting (both within and across products, business lines, or risk factors) and portfolio correlation effects to construct more comprehensive counterparty exposure measures. In such cases, supervisors should ensure that a BO has adequate internal controls governing exposure estimation, including robust model-review processes and data-integrity checks.

When stratifying samples and selecting the counterparties and transactions to use for their targeted testing of practices and internal controls, supervisors and examiners should incorporate measures of potential future exposure regardless of the collateralization of current market-value exposures. As recent events have shown, meaningful counterparty credit risks that surface during periods of stress can go undetected when too much emphasis is placed on collateralization of current market values and only unsecured current market exposures are used for targeting transaction testing.

2126.3.5 CREDIT ENHANCEMENTS

BOs continue to rely increasingly on different types of credit enhancements to mitigate counterparty credit risks. These enhancements include the use of collateral arrangements, contractual downgrades or material-change triggers that enable the alteration of collateral or margining arrangements, or the activation of contractual ''option to terminate'' or closeout provisions.

Collateralization of exposures has become an industry standard for many types of counterparties. Collateralization mitigates but does not eliminate credit risks. BOs therefore should ensure that overreliance on collateral does not compromise other elements of sound counterparty credit-risk management, such as the due-diligence process. Clear policies should govern the determination of loss thresholds and margining requirements for derivatives counterparties of BOs. Such policies should not be so broad that they compromise the risk-reducing nature of collateral agreements with specific types of counterparties. Policies governing collateral arrangements should specifically define those cases in which initial and variation margin is required, and they should explicitly identify situations in which the lack of transparency, business-line risk profiles, and other counterparty characteristics merit special treatment—as may be the case with some highly leveraged counterparties such as hedge funds. Where consistent with the risk profile of the counterparty and instruments involved, policies should specify when margining requirements based on estimates of potential future exposures might be warranted.

Adequate policies should also govern the use of material-change triggers and closeout provisions, which should take into account counterparty-specific situations and risk profiles. For example, closeout provisions based on annual events or material-change triggers based on long-term performance may prove ineffective for counterparties whose risk profiles can change rapidly. Also, such material-change triggers, closeout provisions, and related covenants should be designed to adequately protect against deterioration in a counterparty's creditworthiness. They should ensure that a BO is made aware of adverse financial developments on a timely basis and should facilitate action as counterparty risk increases—well in advance of the time when termination of a relationship is appropriate.

Internal assessments of potential risk exposures sometimes dictate loss thresholds, margining requirements, and closeout provisions with some counterparties. Insufficient internal controls may unduly expose certain BOs to these as well as other types of trading and derivatives counterparties. When evaluating the management of collateral arrangements and other credit enhancements, examiners should not only assess the adequacy of a banking organization's policies but should also determine whether internal controls are sufficient to ensure that practices comply with these policies. Examiners should identify the types of credit enhancements and contractual covenants that are being used when reviewing areas of counterparty risk management, and then determine whether the banking organization has sufficiently assessed the adequacy of these enhancements and covenants relative to the risk profile of the counterparty.

2126.3.6 CREDIT-RISK-EXPOSURE LIMIT-SETTING AND MONITORING SYSTEMS

Exposure-monitoring and limit systems are critical to the effective management of counterparty credit risk. Examiners should focus special attention on the policies, practices, and internal controls employed within such systems at large, complex BOs. An effective exposure-monitoring system consists of (1) establishing meaningful limits on the risk exposures a BO is willing to take, (2) independent, ongoing monitoring of exposures against such limits, and (3) adequate controls to ensure that meaningful risk-controlling action takes place when limits are exceeded. An effective exposure-monitoring and limit process depends on meaningful exposure-measurement methodologies, so supervisors should closely evaluate measurement methodologies, especially for the estimation of PFEs. Inaccurate measurement can easily compromise well-structured policies and procedures. Such situations can lead to limits driven primarily by customer demand and used only to define and monitor customer facilities, rather than limits that serve as strict levels defined by credit management and that initiate risk-controlling actions.

Supervisors and examiners should also assess the procedures used for controlling credit-risk exposures when they become large, when a counterparty's credit standing weakens, or when the market comes under stress. Management should demonstrate its clear ability to reduce large positions. Such actions can include ''capping'' current exposures, curtailing new business, assigning transactions to another counterparty (where feasible), and restructuring the transaction to limit potential exposure or make it less sensitive to market volatility. BOs can also use various credit-enhancement tools to manage exposures that have become unduly large or highly sensitive to market volatility.

2126.3.7 INSPECTION OBJECTIVES

1. To determine if sufficient resources are devoted and adequate attention is given to the management of the risks involved in growing, highly profitable, or potentially high-risk activities and product lines.
2. To ascertain if the banking organization's internal audit and independent risk-management functions adequately focus on growth, profitability, and risk criteria when targeting their reviews.
3. To determine if there is an appropriate balance among all elements of credit-risk management. This balance includes both qualitative and quantitative assessments of counterparty creditworthiness; measurement and evaluation of on- and off-balance sheet exposures, including potential future exposure; adequate stress testing; reliance on collateral and other credit enhancements; and the monitoring of exposures against meaningful limits.
4. To ascertain whether the banking organization employs policies that are sufficiently calibrated to the risk profiles of particular types of counterparties and instruments, which ensures adequate credit-risk assessment, exposure measurement, limit setting, and use of credit enhancements.
5. To ensure that the banking organization's actual business practices conform with their stated policies and the intent of these policies.
6. To establish if the banking organization is moving in a timely fashion to enhance its measurement of counterparty credit-risk exposures, including refining potential future exposure measures and establishing stress-testing methodologies to better incorporate the interaction of market and credit risks.
7. To accomplish the above inspection objectives by using sufficient, targeted transaction testing on those activities, business lines, and products experiencing significant growth, above-normal profitability, or large potential future exposures.

2126.3.8 INSPECTION PROCEDURES

1. Give increased focus to the adequacy, appropriateness, specificity, and rigor of the policies, procedures, and internal controls that a BO currently uses to assess the counterparty credit risks arising from its trading and derivatives activities.
   a. Determine if sufficient written policies cover the assessment of counterparty creditworthiness for the initial due-diligence process (that is, before conducting business with a customer) and for ongoing monitoring.
   b. Give particular attention to how such policies are structured, their adequacy, and how they are implemented.

2. Focus special attention on areas where a BO's practices may not conform to its stated policies.
   a. Determine if the banking organization's policies sufficiently address the risk profiles of its particular types of counterparties and instruments.
   b. Ascertain whether existing practices conform to the stated objectives and the intent of the organization's established policies.
3. Evaluate the banking organization's documentation standards.
4. Determine whether the internal reviews are adequately conducted for business lines, products, and exposures to particular groups of counterparties and individual customers that exhibit significant growth or above-normal profitability.
5. Evaluate the integrity of the internal controls that the banking organization uses to assess its own transaction testing during internal reviews.
6. Conduct independent targeted reviews of the internal controls.
   a. Use robust sampling when testing transactions of major counterparties within a targeted area.

   b. Employ sufficient stratification to ensure that practices involving smaller relationships also adhere to stated policies.
   c. Be alert to situations whereby the current computations of loan equivalents and potential exposures—that are used to measure, monitor, and control derivatives counterparty credit exposures—could be deliberately enhanced.
7. Determine if the banking organization needs to develop more meaningful measures of credit-risk exposures, such as using stress testing and scenario analyses, under volatile market conditions.

2126.5.1 PURPOSE AND BACKGROUND

Section 619 of the Dodd-Frank Wall Street Reform and Consumer Protection Act added a new section 13 to the Bank Holding Company Act of 1956 (BHC Act),[1] commonly referred to as the Volcker rule, which generally prohibits any banking entity from engaging in proprietary trading or from acquiring or retaining an ownership interest in, sponsoring, or having certain relationships with a hedge fund or private equity fund (covered fund), subject to certain exemptions. In 2014, the Board, Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), Securities and Exchange Commission, and Commodity Futures Trading Commission (collectively, the agencies) jointly adopted a final rule implementing these provisions.

The term "banking entity" is defined by statute to include, with limited exceptions

1. any insured depository institution (IDI) (as defined in section 3 of the Federal Deposit Insurance Act (12 U.S.C. 1813));
2. any company that controls an IDI (including a bank holding company (BHC), savings and loan holding company (SLHC), and any other company that controls an IDI but that is not a BHC or SLHC, such as the parent company of an industrial loan company);
3. any company that is treated as a BHC for purposes of section 8 of the International Banking Act of 1978 (for example, any foreign bank operating a branch or agency in the United States); and
4. any affiliate or subsidiary of any of the foregoing (for example, a broker-dealer subsidiary of a BHC) (12 U.S.C. 1851(h)(1)).[2]

The enactment of the Economic Growth, Regulatory Relief, and Consumer Protection Act (EGRRCPA) in 2018 amended the statutory definition of banking entity to exclude certain community banks and their affiliates from the Volcker rule restrictions. Accordingly, in 2019, the agencies adopted amendments to their regulations to exclude IDIs that do not have, and are not controlled by a company that has (1) more than $10 billion in total consolidated assets; and (2) total trading assets and liabilities, as of the most recent calendar quarter, that are more than 5 percent of total consolidated assets.[3]

In 2019 and 2020, the agencies amended their regulations to clarify the proprietary trading and compliance program requirements of the rule, and to clarify the covered funds requirements of the rule, respectively.[4]

2126.5.2 REGULATION VV

Regulation VV, "Proprietary Trading and Certain Interests in and Relationships with Covered Funds," (12 CFR part 248) is the Board's implementing regulation for the Volcker rule. The regulation defines terms used in the statute and related terms, establishes general prohibitions and restrictions on proprietary trading and on investments in or relationships with covered funds, and provides certain compliance program requirements.

Consistent with the statute, Regulation VV exempts from the general prohibitions of the Volcker rule certain activities (for example, market making, underwriting, risk-mitigating hedging, trading in certain government obligations, and organizing and offering a covered fund). However, both the statute and Regulation VV prohibit a banking entity from relying on any exemption to the prohibition on proprietary trading if the permitted activity would involve or result in a material conflict of interest, result in a material exposure to high-risk assets or trading strategies, or pose a threat to the safety and soundness of the banking entity or to the financial stability of the United States.

1. The BHC Act is codified at 12 U.S.C. 1851.
2. Section 13 of the BHC Act also provides that a nonbank financial company designated by the Financial Stability Oversight Council for supervision by the Board (while not a banking entity under section 13 of the BHC Act) would be subject to additional capital requirements, quantitative limits, or other restrictions if the company engages in certain proprietary trading or covered fund activities.
3. See 84 Fed. Reg. 35,008 (July 22, 2019). Consistent with EGRRCPA, the regulation permits an investment adviser that is a banking entity to share a name with a hedge fund or private equity fund that the banking entity organizes and offers under certain circumstances.
4. See 84 Fed. Reg. 61,974 (November 14, 2019) and 85 Fed. Reg. 46,422 (July 31, 2020).

2126.5.3 CAPITAL RULE IMPLICATIONS

Regulation VV provides that a banking entity's aggregate investments in all covered funds pursuant to the exemption for organizing and offering a covered fund may not exceed 3 percent of the banking entity's applicable tier 1 capital (the aggregate funds limitation). Additionally, and consistent with the statute, the regulation requires that a banking entity's investment in a covered fund, including retained earnings, be deducted from tier 1 capital of the banking entity for purposes of determining compliance with applicable regulatory capital standards (the capital deduction requirement).[5] In 2015, the Board, OCC, and FDIC issued guidance to clarify the interaction between the agencies' regulatory capital rules and their regulations implementing the Volcker rule. Refer to SR-15-13, "Supervisory Guidance on the Capital Treatment of Certain Investments in Covered Funds under the Regulatory Capital Rule and the Volcker Rule," and its attachment, "Deduction Methodology for Investments in Covered Funds."

2126.5.4 REQUESTING AN EXTENDED TRANSITION PERIOD FOR ILLIQUID FUNDS

The Board's July 7, 2016, statement entitled, "Order Approving Extension of Conformance Period Under Section 13 of the Bank Holding Company Act," explains that the Board would generally follow a simplified and streamlined process for granting extensions of the holding period for "illiquid funds," as described in this subsection.[6] That process is outlined in SR-16-18, "Procedures for a Banking Entity to Request an Extended Transition Period for Illiquid Funds."

As discussed in the statement, the restrictions and prohibitions of the Volcker rule became effective on July 21, 2012;[7] however, the statute provided banking entities a period of two years until July 21, 2014, to conform their activities and investments to the requirements of the statute and any rule issued by the agencies. Further, the statute provides that the Board may, by rule or order, extend this general conformance period "for not more than one year at a time," up to three times, if in the judgment of the Board, an extension would be consistent with the purposes of the Volcker rule and would not be detrimental to the public interest.[8] On July 7, 2016, the Board issued an order extending the final one-year conformance period for banking entities to conform investments in and relationships with covered funds and foreign funds that were in place prior to December 31, 2013 (legacy covered funds) until July 21, 2017.

The Board also is permitted, upon the application of a banking entity, to provide an additional transition period of up to five years to conform investments in a limited class of legacy illiquid funds.[9] An illiquid fund is defined by the statute as a fund that is "principally invested" in illiquid assets and holds itself out as employing a strategy to invest principally in illiquid assets.[10] The statute provides that this extension applies only to the extent that the banking entity's retention of the ownership interest in the fund, or provision of additional capital to the fund, is necessary to fulfill a contractual obligation of the banking entity that was in effect on May 1, 2010.[11] The statute provides that the Board may grant an extension for each illiquid fund only once and for a period of up to five years.[12] The Board's conformance rule sets forth provisions governing the submission and review of extension requests.[13]

2126.5.5 REQUESTING AN EXTENSION OF THE ONE-YEAR SEEDING PERIOD FOR A COVERED FUND

In 2017, the Board provided guidance to banking entities on the procedures for submitting an application for an extension of the one-year seeding period for a covered fund under the

5. 12 U.S.C. 1851(d)(4)(B); see also 12 CFR 248.12.
6. See Board press release and attachment from July 7, 2016.
7. See 12 U.S.C. 1851(c)(1).
8. See 12 U.S.C. 1851(c)(2). The Board issued rules implementing the Volcker rule conformance provisions in 2011. See "Conformance Period for Entities Engaged in Prohibited Proprietary Trading or Private Equity Fund or Hedge Fund Activities," 76 Fed. Reg. 8265 (February 14, 2011) (12 CFR part 225, subpart K, "Proprietary Trading and Relationships With Hedge Funds and Private Equity Funds," referred to as the "conformance rule").
9. See 12 U.S.C. 1851(c)(3)-(4) and (h)(7).
10. See 12 U.S.C. 1851(h)(7).
11. See 12 U.S.C. 1851(c)(3)(A). In addition, the statute provides that a banking entity may not engage in a prohibited covered fund investment after the date on which the contractual obligation to invest in the illiquid fund terminates. See 12 U.S.C. 1851(c)(4)(A).
12. See 12 U.S.C. 1851(c)(3)(B).
13. See 12 CFR part 225, subpart K.

Volcker rule. Under the statute, a banking entity, regardless of its primary federal financial regulatory agency, must apply to the Board for an extension of the seeding period.

Under the Volcker rule, a banking entity is permitted to acquire and retain an ownership interest in a covered fund in connection with organizing and offering the covered fund as long as certain requirements are met.[14] Section 13(d)(4)(A) of the BHC Act and the Board's Regulation VV permit a banking entity to acquire and retain an ownership interest in a covered fund that the banking entity organizes and offers for the purpose of (1) establishing the fund and providing the fund with sufficient initial equity for investment to permit the fund to attract unaffiliated investors, or (2) making a de minimis investment, subject to several limitations.[15]

The statute and Regulation VV require a banking entity to actively seek unaffiliated investors to reduce its investment in the covered fund, no later than one year after the date of establishment of the fund,[16] to an amount that is not more than 3 percent of the total outstanding ownership interests in the fund (the per-fund limitation).[17] A banking entity may request the Board's approval for an extension of time beyond the one-year period, for up to two additional years, to conform an investment to the per-fund limitation (the seeding period).[18] Under the statute, the Board may grant an extension of the seeding period if the Board finds that the extension would be consistent with safety and soundness and in the public interest.[19]

SR-17-5, "Procedures for a Banking Entity to Request an Extension of the One-Year Seeding Period for a Covered Fund," provides more detailed information on the requirements for submitting such requests and procedures for filing an extension request.

14. See 12 U.S.C. 1851(d)(1)(G) and (d)(4); 12 CFR 248.11(a)-(b).

15. 12 U.S.C. 1851(d)(4)(A); 12 CFR 248.12(a)(1).

16. Regulation VV defines "date of establishment" of a covered fund to mean the date on which the investment adviser or similar entity to the covered fund begins making investments pursuant to the written investment strategy for the fund. In the case of an issuing entity of asset-backed securities, the date of establishment is the date on which the assets are initially transferred into the issuing entity of the asset-backed securities. See 12 CFR 248.12(a)(2)(iv).

17. See 12 U.S.C. 1851(d)(4)(B); see 12 CFR 248.12(a)(2). Regulation VV permits a banking entity to hold a greater amount of a covered fund under the per-fund limitation if required in order to meet the risk retention requirements of section 15G of the Securities Exchange Act and implementing regulations. See 12 CFR 248.12(a)(2)(ii)(B).

18. See 12 U.S.C. 1851(d)(4)(C); 12 CFR 248.12(e).

19. See 12 U.S.C. 1851(d)(4)(C). In their regulations, the agencies recognized the potential for evasion of the restrictions contained in the Volcker rule through misuse of requests for extensions of the seeding period for covered funds and stated that the Board and the other agencies would monitor requests for extensions of the seeding period for activity in covered funds that is inconsistent with the requirements of the Volcker rule. See 79 Fed. Reg. 5725 and 5736 (January 31, 2014).

WHAT NEW IN THIS REVISED SECTION

Effective January 2010 this section was revised to include a brief overview of the January 6, 2010, interagency advisory on interest-rate risk management that targets interest-rate risk management at insured depository institutions. The advisory does not constitute new guidance. The principles and supervisory expectations discussed within the guidance apply also to bank holding companies, which should manage and control aggregate risk exposures on a consolidated basis. See SR-10-1.

2127.0.1 ASSESSING THE MANAGEMENT AND INTERNAL CONTROLS OVER INTEREST-RATE RISK

Interest-rate risk (IRR) is the exposure of a banking organization's financial condition to adverse movements in interest rates. Accepting this risk can be an important source of profitability and shareholder value. However, excessive levels of IRR can pose a significant threat to a bank's or bank holding company's (BHC's) earnings and capital base. Accordingly, effective risk management that maintains IRR at prudent levels is essential to the organization's safety and soundness.

Evaluating a BHC's exposure to changes in interest rates is an important element of any full-scope inspection and may be the sole topic for specialized or targeted inspections. This evaluation includes assessing both the adequacy of the management process used to control IRR and the organization's quantitative level of exposure. When assessing the IRR management process, examiners should ensure that appropriate policies, procedures, management information systems, and internal controls are in place to maintain IRR at prudent levels with consistency and continuity. Evaluating the quantitative level of IRR exposure requires examiners to assess the existing and potential future effects of changes in interest rates on a BHC's consolidated financial condition including its capital adequacy; earnings; liquidity; and, where appropriate, asset quality. To ensure that these assessments are both effective and efficient, examiner resources must be appropriately targeted at those elements of an organization's IRR that pose the greatest threat to its financial condition. This targeting requires an inspection process built on a well-focused assessment of IRR exposure before the on-site engagement, a clearly defined inspection scope, and a comprehensive program for following up on inspection findings and ongoing monitoring.

2127.0.2 JOINT AGENCY POLICY STATEMENT: INTEREST-RATE RISK

The Board, together with the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation, adopted a May 23, 1996, Joint Agency Policy Statement on Interest-Rate Risk, effective June 26, 1996. (See SR-96-13.) It provides guidance to examiners and bankers on sound practices for managing IRR, which form the basis for ongoing evaluation of the adequacy of IRR management at supervised institutions.

The policy statement outlines fundamental elements of sound management that have been identified in prior Federal Reserve guidance and discusses the importance of these elements in the context of managing IRR.[1] Specifically, the guidance emphasizes the need for active board and senior management oversight and a comprehensive risk-management process that effectively identifies, measures, and controls IRR.

Although the guidance targets IRR management at commercial banks and Edge Act corporations, the basic principles presented in the policy statement are to be applied to bank holding companies (BHCs). BHCs should manage and control aggregate risk exposure on a consolidated basis by recognizing legal distinctions and possible obstacles to cash movements among subsidiaries. The assessment of interest-rate risk management made by examiners in accordance with the 1996 Joint Policy Statement will be incorporated into a BHC's overall

1. Guidance to examiners identifying fundamental elements of sound risk management includes SR-00-14, "Enhancements to the Interagency Program for Supervising the U.S. Operations of Foreign Banking Organizations"; SR-96-14 (see section 2124.0), "Risk-Focused Safety and Soundness Examinations and Inspections"; SR-96-13, "Joint Policy Statement on Interest-Rate Risk"; SR-96-10, "Risk-Focused Fiduciary Examinations"; SR-95-51 (see section 4070.1), "Rating the Adequacy of Risk-Management Processes and Internal Controls at State Member Banks and Bank Holding Companies"; and SR-93-69 (see section 2125.0), "Examining Risk Management and Internal Controls for Trading Activities of Banking Organizations."

risk-management rating. BHC examiners should refer to section 4090.1 of the *Commercial Bank Examination Manual* for more detailed inspection guidance on the joint policy statement on IRR.

2127.0.3 INTERAGENCY ADVISORY ON INTEREST RATE RISK MANAGEMENT

A January 6, 2010, interagency advisory was issued by the Board of Governors of the Federal Reserve System and other federal regulators[2] that reminds institutions of supervisory expectations on sound practices for managing IRR. The advisory does not constitute new guidance. It reiterates basic principles of sound IRR management that each of the regulators has codified in its existing guidance, as well as in the interagency guidance on IRR management issued by the banking agencies in SR-96-13. The advisory highlights also the need for active board and senior management oversight and a comprehensive risk-management process that effectively measures, monitors, and controls IRR.

The advisory targets IRR management at insured depository institutions. However, the principles and supervisory expectations articulated also apply to BHCs, which are reminded of long-standing supervisory guidance that they should manage and control aggregate risk exposures on a consolidated basis while recognizing legal distinctions and possible obstacles to cash movements among subsidiaries. See SR-10-1.

2 The other financial regulators include the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision (OTS), and the Federal Financial Institutions Examination Council (FFIEC) State Liaison Committee (collectively, the regulators).